TOTAL SURVEILLANCE

How today's digital mass surveillance

threatens free societies

MULLVAD VPN

TOTAL SURVEILLANCE

How today's digital mass surveillance
threatens free societies

MULLVAD VPN

CONTENTS

Second edition. Printed in Sweden, August 2024

Commercial mass surveillance

State mass surveillance

The consequences of mass surveillance

PREFACE

We live in a world where everything we do on the internet is tracked and saved (if we don't oppose with privacy-focused services). An infrastructure has been constructed that means the tech giants can follow your every move. And where your innermost thoughts (in other words, what you google) are no longer your own. This has been going on for more than 20 years now and we're starting to see how serious the consequences are.

Some of the world's biggest tech companies have been allowed to collect extremely personal data about almost everyone in the world. They do this via social media and via apps. But above all they do it via every single website you visit. You don't even need to have downloaded the Facebook app for Meta to know exactly who you are.

And it isn't just the tech giants that act like this. Try reading the small print next time you visit a new website. There are hundreds – sometimes thousands – of actors there, just waiting to record what you're doing. Most of them are what's known as data brokers, and these companies have a single purpose. Collecting data about you so they can repackage it and sell it on. This is actually illegal, and Meta and Google have had to pay heavy fines for doing it. So the question is why it's still happening. Well, the short answer is that too many companies are interested in making money from it. And too many states are interested in using the collected data to achieve political influence and control.

In 2013, Edward Snowden revealed how the USA was carrying out mass surveillance on both foreign and American citizens – surveillance that the American federal court determined was illegal. And although Snowden was a whistleblower who revealed that the USA had been breaking the law, he is so fearful of the consequences that he cannot return to his home country. As recently as spring 2024, the USA extended the exemption that breaks their own constitution, making it possible for the country to map every single person on the planet.

In Europe, the European Commission and parts of the Council of Ministers have attempted to introduce 'chat control', steamrollering both the European Court of Justice and human rights. This happens over and over again – authorities infringe the human rights that entitle each of us to privacy. At least five EU countries have been found to use Pegasus spyware against dissenters. And yet they claim they have the right to exercise mass surveillance on the basis that "if you have nothing to hide, you have nothing to worry about".

Yet we can already see how collected personal data is being used in campaigns to influence elections. We are feeling the consequences of these actions, here and now. But the really big question is where we'll end up if we don't stop this abuse. In China, we can see how mass surveillance is used to control the population, to persecute anyone critical to the state and to build social score systems. There, the future looks like the script of a dystopian movie. And that's where we're headed. If democratic countries think they can just keep moving the boundaries, they're wrong. Ultimately all that remains is total monitoring and total control.

Personal integrity is the right on which all other rights rest. If we don't have the right to explore new thoughts and ideas without someone constantly registering that process, if we don't have the right to private conversations with those close to us, if we don't have the right

to decide for ourselves when and to whom we express something – do we even have free speech at all? Freedom of speech means the right to say what you want, but it should also mean the right to decide when and to whom you say it. If we have no right to a private life, we have lost the right to be independent humans.

And to anyone saying they have nothing to hide – this isn't about you. It's about all of us. It's about the people who really do have something to hide. Activists under oppressive regimes, whistleblowers, journalists, advocates working for human rights, vulnerable people, statesmen and women with secret information vital to the security of the nation, innovators with pioneering ideas... And many, many more. Above all, it's about the impact of data collection on entire societies in the long run and what it does to us as human beings. It's about all our futures too. About the generations to come. And whether they will grow up in a free or controlling society.

It's time for the world's politicians to get to grips with the basic problem. It doesn't matter if a certain tracking method (such as third-party cookies) is banned, as the major data collectors constantly turn to new technologies. A bigger change is needed. Collecting and selling or sharing personal data must be prohibited. We must discard business models based on people's behavioral data. We must also make government agencies accountable for their violations of the law. We must vote for politicians who care about constitutions and human rights conventions. In many respects, democratic societies are based on the fact that we set limits on those in power. And we have done so for a reason. As long as those limits continue to be broken, Mullvad will offer technical resistance.

Jan Jonsson
CEO, Mullvad VPN

COMMERCIAL MASS SURVEILLANCE: THE BUSINESS MODEL

The tech giants know everything about you – whether or not you use their services.

Your online behavior is the raw material from which one of the biggest economies in the history of the world has been built. But it isn't the images you post, the comments you write or the messages you send that are the hard currency. It's the data about the data that's the true treasure. With what's known as metadata, the tech giants aren't satisfied with monitoring your life – they've decided to control it.

The internet has developed into an infrastructure where it's pretty much possible to find out anything about anyone, any time. And this isn't merely theoretical speculation, but a possibility that's exploited every day. Surveillance has become the motor for the World Wide Web. Mapping everyone on Earth has produced one of the fattest cash cows in world history. This may sound a bit exaggerated coming from a company offering services for online privacy, but the fact is that this is what the harsh reality looks like. Every step we take is fed

into huge systems where AI and machine learning is used to register, categorize and calculate what we'll do next.

Essentially, there are two types of organizations carrying out mass surveillance in the digital world: those monitoring people to earn money (tech companies) and those monitoring people to control them (states). Often, their paths cross – not least when the latter step in and root around in the tech companies' data storage. We will come back to the state surveillance later, but let us now start with those who collect large amounts of data for commercial purposes.

Let's start with the obvious stuff. The tech giants companies log your activity on their platforms to earn money. If you have a Facebook account, Meta collects data on your activity there, and if you use Messenger, Meta saves the private messages you write to family and friends[1] (unless you click on end-to-end encryption, which they've launched recently). If you use Google's services – for example if you send an email with Gmail or login to YouTube to check out a video – Google saves and categorizes everything you do, because you're on their platforms. When you use apps on your phone, they of course log your activity too. And social networks freely swap this information back and forth between each other.[2] Among other leaks, it's been revealed that Meta leaked personal conversations to some of the 150 partners[3] who seem to fall outside the privacy rules the company set up after the Cambridge Analytica scandal.[4] These are collaborations that aren't visible on the surface and which you can't control in the user settings[5], but which often only come to public notice during leaks, trials and questions to congresses or parliaments. The collected data is used to tailor your filter bubble and to target information and advertising to you. As we've already said, this is obvious. This is the data you transfer when you accept the terms of use. It's just as obvious that you can choose not to use this type of service. Of course there are alternative social media channels that have chosen another way (they

aren't exactly numerically superior right now, but they do exist). For example, you can choose the messaging service Signal[6] if you want to communicate privately. But the huge problem with today's widespread data collection is that you don't even need to be active on the major services to contribute big data to big tech.

It's enough to simply surf with a normal web browser to contribute to data collection.

The collected data that comes from your activity when you're logged in on social media is just the tip of the iceberg. The really big data collection – the one that grinds along day in, day out and registers everything you do – continues regardless of whether or not you choose to use Facebook and Google. You could have avoided Meta your entire life – it still knows everything about you. It's enough to simply surf with a normal web browser to climb aboard this carousel. But how is that possible? Meta actually reveals the method right there in its name. The technology it uses is metadata.

> **"Metadata made it technically possible to rewind the events in someone's life going back months or even years."**
>
> Edward Snowden

In 2012, something happened that changed both how Edward Snowden viewed his employer (the NSA, which is responsible for foreign signals intelligence in the USA) and how he viewed the world around him. The governments in Australia and the UK proposed to make it mandatory to register metadata on the internet. In his book Permanent Record, he describes how "this was the first time that notionally democratic governments publicly avowed the ambition to establish a sort of surveillance time machine, which would enable them to technologically rewind the events of a person's life for a period going back months or even years". Snowden argues that it was a final mark of the western world's transformation from being a creator and defender of the free internet to becoming its opponent and future destroyer. But to paraphrase the current NSA: it was only metadata.

So what is metadata? Bruce Schneier, a leading American cryptographer and security expert, describes it as data about data. In his book Data and Goliath, he writes:

"In a text message system, the messages themselves are data, but the accounts that sent and received the message, and the date and time of the message, are all metadata. An e-mail system is similar: the text of the e-mail is data, but the sender, receiver, routing data, and message size are all metadata. Metadata may sound uninteresting, but it's anything but."

After Snowden leaked the NSA documents, Bruce Schneier worked with one of the journalists who was there in that hotel room in Hong Kong: Glenn Greenwald from the Guardian. Schneier helped Greenwald analyze the more technical parts of the leaks, and as he did so described the problem of dismissing metadata as something non-personal.

"One government defense is that the data collected is 'only metadata'. This seemed to mollify many people, but it shouldn't have.

Collecting metadata on people means putting them under surveillance."

Bruce Schneier compares it to hiring a private detective. A private detective can bug their target: listen in on everything the person says in their home, during their phone calls and so on. That's data. But then the private detective can also choose to carry out surveillance on their target. And that produces a different type of report. Who the person meets, where they go, where they spend time, which people they write to, what they read and buy. That's metadata.

"Eavesdropping gets you the conversations. Surveillance gets you everything else," writes Schneier. "Metadata reveals our intimate friends, business associations. It reveals what and who we're interested in and what's important for us, no matter how private."

"Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."

Former NSA general counsel Steward Baker

The collection of metadata for commercial purposes means the tech giants can map your entire life. Essentially, metadata makes it possible to keep track of all the sites you visit, all the searches you do, all the people you talk to, how often you talk to them and for how long. In addition to this, the tech giants have the technical skill and not least the will to log everything on detail level as well: exactly what you buy online, which ads you look at, which products you like and which ones you quickly scroll past, which texts you read and which videos you watch (and once again, how often and for how long). And they have access to all this regardless of whether or not you're logged into their services, because the internet's infrastructure means that essentially every site in the world collaborates with the tech giants for commercial purposes.

Stewart Baker, former general counsel for the NSA, expressed this clearly[7]: "Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."

His colleague Michael Hayden, former director of the NSA and CIA, agrees, and in a debate at John Hopkins University[8] referred to Baker when he said: "Baker is absolutely right. We kill people based on metadata."

"We don't lie to our search engine. They know more about what I'm thinking of than I do."

As we said before, this article isn't about state mass surveillance, but we think state representatives provide a clear picture of what metadata is and how accurately it can be used. It's also important to emphasize this: the NSA categorizes search histories as metadata. Bruce Schneier says you can argue whether data from search engines is data or metadata, but the fact that NSA categorizes it as metadata should suffice to dismiss their 'It's only metadata' argument.

"We don't lie to our search engine," says Schneier. "Google knows what kind of porn each of us searches for, which old lovers we still think about, our shames, our concerns, and our secrets. If Google decided to, it could figure out which of us is worried about our mental health, thinking about tax evasion, or planning to protest a particular government policy. I used to say that Google knows more about what I'm thinking of than my wife does. But that doesn't go far enough. Google knows more about what I'm thinking of than I do, because Google remembers all of it perfectly and forever."

Leah Elliott, who's a satirical cartoonist and digital rights activist, is thinking along the same lines. In her series Contra Chrome[9] – How Google's Browser became a threat to privacy and democracy – she expresses it like this:

"You think you are browsing the web, when in reality, Google and others are browsing you. Extracting your experiences without your awareness, your knowledge, or your consent."

Bruce Schneier's comparison with a private detective is good, but it's not quite sufficient, because the life we live digitally isn't totally comparable with the life we live in the physical world. Because what we search for in search engines and on the sites we visit reflects our thoughts in a way that our physical behavior doesn't. The internet has reduced the distance between thought and action in a way that has no equivalent in the physical world. If we're worried that we drink too much, we can google it; we don't need to go out and throw away all the whiskey bottles in the garbage, sneakily read a book on the subject at the library or go to a physical meeting with the private detective on our heels. Mapping people online means invading their heads and reading their thoughts before they blossom and become actions.

In the same way, metadata isn't entirely comparable with the direct conversations we have online. There are parts of your life that

you're perhaps not ready to write or talk about with other people, but which you explore in private. Metadata even makes it possible to detect things we perhaps don't even know about ourselves. Minor changes in the types of food you search for can indicate that you're pregnant even before you've done a test. Metadata also equates to collection of data that isn't legal in many countries. For example recording your political, sexual or religious orientation. If you visit your church website every Sunday, it's probable you belong to that religious community. This is data that the tech giants have on you, but which is prohibited by law. The tech companies hide behind the argument that 'it's only metadata' and that it's anyway it's anonymous data – but in the fraction of a second, this information could be de-anonymized and linked to you personally.

In the documentary The Big Data Robbery[10], Harvard professor Shoshana Zuboff calls metadata 'waste'.

"Back in the year 2000, these data were considered just extra data. People called them things like data exhaust. Eventually it was understood that these so-called waste materials harbored these rich predictive data."

This insight completely transformed the internet. The way people surfed became the true treasure, and the tech giants made a fortune from metadata. But it isn't only the known large companies who are getting in on the new digital marketplace. For example, the new economy has attracted data brokers who grab a slice of the cake by simply collecting, buying and selling data about the sites people visit, the searches they do and so on.

“Right from the start, they understood that these mechanisms had to be hidden. They had to observe through a one-way mirror. That’s what makes it surveillance.”

Shoshana Zuboff

Zuboff calls the internet's new infrastructure 'Surveillance Capitalism'. Capitalism because they make money from mapping people's behavior on the internet. Surveillance because they observe us in secret and use methods developed to prevent us becoming aware of them.

"The companies like to say 'We collect data so that we can improve our service', and that's true. They collect data and some of it is used to improve the service to you. But even more of it is analyzed to train what they call models, patterns of human behavior. So once I have big training models, I can see how people with these characteristics typically behave over time, and that allows me to fit your data right into that arc and predict what you're likely to do, not only now but soon and later. This is what I call behavioral surplus; these data streams filled with these rich predictive data. Why surplus? Because right from the start these were more data than was required to improve products and services."

Your behavior on the internet is sold to both banks and insurance companies.

In her book The Age of Surveillance Capitalism, Zuboff writes that the tech giants realized at an early stage that they would have to conceal their business model. In an interview in Contagious Magazine[11] she explained her reasoning.

"Google understood that just grabbing your experience, bringing it into data for their own systems of production and sales, was not going to sit well with people. So, right from the start, they understood that these mechanisms had to be hidden. They had to observe through a one-way mirror. That's what makes it surveillance."

The actual mechanism is concealed. It's hidden in hundreds of policy pages that nobody can be bothered to read (it's much easier to just press 'Accept' when the cookie question pops up). Or not even known: like when Meta refuses to explain what data it collects, even

when a court asks it.[12] But the tech giants have been extremely transparent about the actual philosophy behind surveillance capitalism, right from the start. Mark Zuckerberg has talked about how privacy is no longer a social norm.[13] Or when Eric Schmidt, Google CEO during the period 2001–2011, expressed it like this in an interview[14]:

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

The funny thing was that Schmidt then blacklisted American media website CNET[15] because their journalists had revealed information about Schmidt in an article. Information they'd discovered simply by Googling.

An even clearer statement and proof of Google's attitude in the early 2010s came in another interview[16] where Schmidt said: "We know where you are. We know where you've been. We can more or less know what you're thinking about."

Since then, the quantity of data collected has only increased. As Tristan Harris, former design ethicist at Google and later founder of The Center of Humane Technology[17], expressed it in the documentary Social Dilemma[18]: "They know when people are lonely. They know when people are depressed. They know when people are looking at photos of your ex-romantic partners. They know what you're doing late at night. They know the entire thing. Whether you're an introvert or an extrovert, or what kind of neuroses you have, what your personality type is like."

“We build systems that spy on people in exchange for services. Corporations call it marketing.”

Bruce Schneier

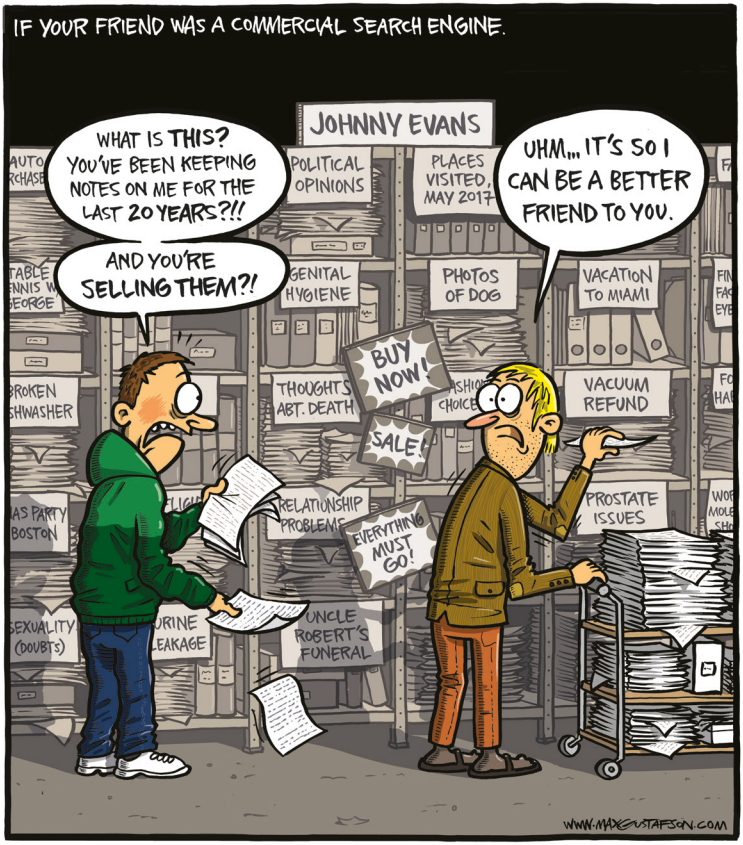
Just like Shoshana Zuboff, Bruce Schneier is careful to point out this business model as surveillance and nothing else.

“Corporations call it marketing, but it’s surveillance. Surveillance is the business model of the internet. We build systems that spy on people in exchange for services.”

Surveillance is ultimately about control – that’s the whole point of it. And it’s clear that the business model prevailing on the internet today isn’t merely about observing. The infrastructure that’s been built makes it possible to use what Zuboff calls ‘future behavior’ to steer people in the direction you want. Behavioral data has become the tool used to tilt people in different directions, for financial or political gain. Zuboff says the tech giants have gone from monitoring to activating.[19] In her book The Age of Surveillance Capitalism, she writes:

“Automated machine processes not only know our behavior but also shape our behavior at scale. With this reorientation from knowledge to power, it is no longer enough to automate information flows about us; the goal now is to automate us. Today’s prediction products

are traded in behavioral futures markets that extend beyond targeted online ads to many other sectors, including insurance, retail, finance, and an ever-widening range of goods and services companies determined to participate in these new and profitable markets. In the thousands of transactions we make, we now pay for our own domination."



COMMERCIAL MASS SURVEILLANCE: THE ACTORS BEHIND THE DATA COLLECTION

Here are the companies mapping your life.

Part 1: Big Tech – they've collected so much data about you that they've lost control.

You already know which big companies collect data for commercial purposes. But the question is whether you're aware of the absurd extent of this data collection. You can take as long as you like to think about it, but the answer is still 'No'. Not even the companies themselves know how much data they collect, where it goes and how they should control it.

Mapping human behavior on the internet through collection of data that's in fact extremely private has formed the basis for one of the world's biggest economies. We will later explain how the actual data collection is done, and what the data is used for. But first, let's take a moment to identify which tech companies run this marketplace of behavioral data that the internet has been transformed into – and to look at the absurdly large amounts of data they collect.

Let's start with the internet service providers. It's pretty obvious that they keep track of what you do online (unless you're using a VPN,

of course). Nor is it particularly strange that they do this, because in many countries they're forced to log your traffic by law. That doesn't mean all internet service providers make an extra buck by selling the data on – but in a country like the USA it's extremely common.[20] An investigation by Vice discovered that it was even possible to buy people's geographical location in real time.[21] And according to a report by the Federal Trade Commission (FTC) in the USA, at least six of the largest internet service providers map their customers' internet behavior[22] and their alternatives for offering their customers privacy are an illusion.

So what else is there? Payment services: For example, Paypal has been reported to have terms and conditions that are longer than Shakespeare's Hamlet[23], which gives a good indication that their data collection is somewhat excessive. The apps in your phone: Washington Post journalist Geoffrey A. Fowler calculated the total number of words in his phone's privacy policies[24] and they added up to around 1 million – or twice as long as Tolstoy's War and Peace, if we're going to continue the comparison with classic literature. And yes, user agreements this long equals data collection. When it comes to the apps, location data is one of the most attractive items. And in this particular category, there's no limit on the sensitivity of the data[25] that's sold to the highest bidder; visits to medical clinics and religious institutions are amongst the basic products in a marketplace where people's physical movement patterns bring in 12 billion dollars a year.[26] And don't think you're immune because you've switched off location services. For the sake of simplicity, let's use Meta as an example. Its business model includes paying its way out of court cases. This is no problem for it financially, but for every settlement we get to know a bit more about its methods. In a single agreement in 2022, for example, it paid 37 million dollars after having tracked 70 million users[27] despite them rejecting the location service function. Still more expensive

was the settlement with those affected by the Cambridge Analytica leaks, where Meta agreed to pay 725 million dollars[28] after leaking data including private conversations. Meta in itself deserves a more exhaustive presentation. You'll probably agree when you've read the next few paragraphs.

Meta – doesn't even know itself how much data it collects, where it goes or how it could be deleted.

Both Google and Meta offer you as a user the opportunity to control and review the data collected by the company about you. But this is a false impression, and far from the entire truth. Meta doesn't even want to reveal in court how much data it has. In a hearing linked to the Cambridge Analytica scandal[29], the company agreed to share data that can be found under 'Download Your Information' but argued that it wanted to keep data from 'non-consumer parts of Facebook' outside the courtroom. When the court didn't agree with this and demanded an answer from two of Meta's heads of development, they answered that not even Meta knows exactly how much data it has on people. "I don't believe there's a single person that exists who could answer that question."[30]

In spring 2022, leaked documents gave the same picture when employees at Meta admitted that "We do not have an adequate level of control and explainability over how our systems use data".[31] Vice magazine published parts of the leak where employees at Meta compared its system with pouring ink in water.

"We've built systems with open borders. Imagine you hold a bottle of ink in your hand. This bottle of ink is a mixture of all kinds of user data: third-party data, first party data, sensitive data. You pour that ink into a lake of water (our open data systems; our open culture). And it flows everywhere. How do you put that ink back in the bottle?

How do you organize it again, such that it only flows to the allowed places in the lake?"

The image emerges of a Meta without control over its (your) data. All that remains is to try and work out how much data it actually has. Over the years, there have been indications that the quantity is quite simply absurd. When ProPublica mapped Facebook's data collection, it turned out that as early as 2016, Meta had a dizzying 52,000 unique attributes[32] which it used to categorize people with the help of machine learning. Meta certainly wants to give the impression that the data collection primarily comes from users' activity on their platforms. But you only have to read about scandal[33] after scandal[34] after scandal[35] where Meta and data leaks have gone hand-in-hand to get a completely different picture. The leaks are often linked to the technology that they once called Facebook Pixel; the ad system that billions of sites use and which makes it possible for Meta to reach far beyond its own apps when it feeds its AI and machine learning systems with data.

Meta collects information about customers who've bought pregnancy tests and sought consultations for erectile dysfunction. This applies to people all over the world, regardless of whether or not they have a Facebook account.

To put it simply, Meta's Pixel system means websites give Meta access to how their site visitors behave – what they buy, what they avoid, what texts they read, what videos they look at and so on – and in

return the sites get to use Meta's total data collection to optimally tailor and target their ads (on Meta's platforms and in its ad system). In an investigation by The Markup[36] it emerged that one in three of the world's most popular 100,000 websites were linked to Meta Pixel. It's this infrastructure that means Meta can keep track of internet users all over the world, regardless of whether or not they have a Facebook account.[37]

When a leak via Meta Pixel is revealed, the newspaper headlines are often about how it has been possible to link sensitive purchases or online behaviors to real people via email addresses or phone numbers. For example, it has emerged that the Pixel technology registers data about pharmacy customers who bought HIV tests, pregnancy tests and who sought consultations for erectile dysfunction.[38] But there's actually no difference between a 'scandalous leak' where personal data such as email addresses has been leaked together with online behavior, and the constant flow of collected data that tech companies suck in every day, where the data can be linked to people with other methods: using IP addresses, cookies and other techniques. It doesn't matter how much the tech giants excuse their actions by saying the data they have for profiles is anonymized. You only need enough data about someone for it to be impossible to keep it anonymous. It takes no time at all to put together the jigsaw revealing who's hiding behind the data – and then it's de-anonymized. Particularly if your entire business model is based on huge AI and machine learning systems whose only purpose is to categorize everything an individual does to build a profile of them.

Even though Meta has access to data about its 2 billion users and also tracks people on every third site in the world, the company isn't satisfied with that. As well as collecting its own data, it also buys extra data from what are known as data brokers.[39] It has also been revealed to have bought up VPN company Onavo to use it as spyware.

In other words, from the outside it looked like Meta was entering the privacy world. But this wasn't the case – yet one more reason why it's important to choose your VPN service carefully. Instead the VPN service was used for completely different purposes. The users who downloaded Onavo got spyware installed on their phones[243]. And by using hacking techniques, Meta made sure that their VPN app picked up data from other apps. The main aim was to access encrypted traffic from its competitor, Snapchat.

The total amount of data collected gives Meta the ability – which it described in leaked documents[40] – to target ads at people based on how they will behave, what they will buy and what they will think.

The scandals, the leaks and the absurd figures about how much data Meta actually collects gives us a good image of the company. But what perhaps says most about the company's values and ambitions are the approaches it uses. It's in the technical details that it becomes clear surveillance is the true core of Meta's business model.

Meta collects the movements you make with your mouse, the messages you've written on social media but never posted and how you move when you carry your mobile phone, even when you've clicked to refuse sharing location data.

Meta isn't exactly known for being transparent about how the company collects data and what it does with it. But you can use a back door to get into its thinking by reading its patents. It calls one of them Offline Trajectories[41,] and it's about using techniques that can predict when you're about to lose signal and go offline. Several of the company's

patents relate to this – in other words, finding ways to locate you even if you resist. One patent is called Location Prediction Using Wireless Signals on Online Social Networks[42], and just like it sounds, it's all about using the strength of your Wi-Fi connection or reading your Bluetooth to locate you. In the same way, Meta has used other people's mobiles (near you) to identify your position even when you have location data switched off. Meta has been sued for breaking Apple's Tracking Transparency[43] and has itself admitted it can track people even when location services are switched off.[44]

But nothing has revealed the extent of Meta's data collection as clearly as the aftermath of the Cambridge Analytica scandal[45], where 87 million users' metadata and personal messages went straight to an analysis company using the information to affect the American presidential election. Amongst other things, it emerged[46] that Meta reads and registers your movement patterns with your computer mouse and the public Wi-Fi networks in proximity to tracked mobile phones. They use mobile masts and GPS to work out where you are. And they log your battery percentage, available storage space, installed plug-ins and the speed of your connection to identify you. The company also admitted that it uses metadata from images you take with your phone (data that isn't visible to the naked eye but which is embedded in the pictures) to identify and track you. Spokespeople for Meta also confirmed it registers IP addresses and purchases data from data brokers to build clearer personal profiles.

Meta's patents reveal the core of its business model and its ultimate ambitions. One of the patents even aims to predict when you're going to die.

Meta has also been exposed for using something called the accelerometer to track people[47]; this is the hardware in your phone that measures your movements and direction and which means, for example, that your phone can switch between vertical and horizontal mode. By mapping movement patterns and linking them to other apps on your phone, Meta has been able to identify how you move and when you visit different types of places. This technology has even been used to match with mobiles close to you, and suddenly it becomes extremely clear that the tech companies have access to technologies far beyond the obvious in their hunt for personal data. In another invasive way, Meta has monitored what people have written but not posted[48] in different online forms. Meta calls these unposted thoughts 'self-censorship'. We'll say that again – text you wrote but that, for whatever reason, you chose not to post, has been saved and logged by Meta. But none of this truly comes as a shock any more. Meta also has patents for technology that can predict when people go through 'life changing events' by analyzing everyday routines and how your sleep changes (with your phone on your nightstand, everything's possible). The patent even aims to predict when you're going to die.[49] Welcome to a brave new world.

Google – with a monopoly in terms of both search engine and web browser, it knows everything about everyone.

Of course, even if Meta appears to be extremely good at data collection, it faces stiff competition in Google. While Meta Pixel is present on one in three sites, Google's equivalent, Google Analytics, manages 74%.[50] The way it works is roughly the same. When a website has Google Analytics installed – to measure and analyze the traffic on the website and link it to Google's ad system for more accurate marketing – Google also gets access to how visitors behave. But that isn't the only tool in

Google's belt. The company also provides free fonts for websites. This is an offer that 60 million sites have found difficult to refuse. And just like the company's analysis tool, these come with the same demand for something in return: that Google can collect information about site visitors. On websites using Google Fonts, it can monitor visitors and how they behave by registering their IP address[51] and then cross-referencing it with all the other information it has that's connected to that particular IP address. The same sort of collection takes place wherever there's a Google search box embedded in a website (this also applies wherever there's a 'share' button from Facebook, Twitter or Instagram). Overall, this gives Google an enormous flow of data. But we all know this is only the start.

In 2022, Google paid 400 million dollars in a single settlement – then carried on with its core business: collecting personal information.

9 out of 10 people who use a search engine[52] do so by googling. This means Google has an insight into the inmost thoughts and life of virtually every internet user in the world. And it doesn't even end there. 7 out of 10 browsers[53] used today are Google's Chrome, a browser used to google you rather than you using it to look things up.[54] Add YouTube and Gmail, and what Google knows about the world and its inhabitants is almost limitless.

Just like Meta, Google has a huge budget for legal settlements[55] (in a single settlement in 2022, it laid out a cool 400 million dollars – before continuing to collect data as before). Google has the ability to buy its way out, but the legal pressures have not left the tech giant completely unaffected. Google Analytics has essentially been outlawed

in several countries[56], and third-party cookies have been under legal pressure[57], which has led Google to at least attempt to phase out that type of data collection. The only problem is that big tech is faster than lawmakers. It doesn't matter if companies like Google remove a specific tracking technique, because they always find new ways to collect data.[59] Since it's their core business. As Larry Page, one of Google's founders, said in an interview way back in 2001[60]: "Personal information is Google's business."

In recent years, Google has felt forced to take a number of measures to appear as if it cared about privacy, despite the fact that its entire business model is built on exactly the opposite. For instance, it has announced that it deletes data after 18 months.[61] If we ignore the fact that this means your digital footprint will be saved for 18 months at a time, the obvious question is 'Does it really matter what Google say it's doing?' When Washington Post journalist Geoffrey A. Fowler contacted Google and asked why it was keeping 167 Gb of data about him – or 83,500 Stephen King novels, if you prefer – the company's answer was merely: "We've long focused on minimizing the data we use to make our products helpful."[62] When the abortion laws were changed in the USA, Google said it would proactively delete 'particularly personal' data about the places people visited[63], such as abortion clinics and hospitals. A year after this statement, nothing had changed.[64] It's worth repeating: personal information is Google's business. This means it can't entirely ignore the world around it. But it does also mean that it'll probably continue handling new legal requirements and pressure from the public by trying to find new ways of collecting data. At least until it changes its business model.

There are more tech companies that deserve a mention. TikTok has been accused of collecting large quantities of data[65] and sharing it with the Chinese state. It is also clear on its own site that it collects things like keystroke patterns and the rhythm in how you write.[66]

Amazon has been exposed collecting absurdly large amounts of data in both its digital ecosystem[67] and in physical stores.[68] And you really don't want to know where your credit card transaction data goes.[69] As we've already said, the vast majority of the internet has been transformed into an infrastructure where the collection of personal data is used to increase both revenues and power. And it's going to take strong resistance to overturn that trend.

COMMERCIAL MASS SURVEILLANCE: THE ACTORS BEHIND THE DATA COLLECTION

Here are the companies mapping your life.

Part 2: Data brokers – you've never even heard of them. They know almost everything about you.

It's not just the tech giants that carry out commercial mass surveillance. There are companies working in the shadows, with a single purpose: to collect, buy and sell data about your online activities. And the lists they offer for sale don't make pleasant reading.

If you visit a website for the first time and instead of clicking Accept, click Manage cookies when that infuriating cookie warning pops up, you can go through a list of the (often) hundreds of companies that have cookies or other tracking technologies represented on that site. You'll probably expect to find companies like Meta and Google here, and you will – together with several other world-leading companies like Amazon, X, Microsoft and so on. But if you scroll a couple more times, names start to appear that don't sound quite as familiar: Kochava, Veraset, Cuebiq, Spectus, X-Mode... and the list is practically endless. These are what are known as data brokers. Companies that exclusively devote themselves to one single thing: collecting, buying and selling information about your internet behavior.

In other words, data brokers don't offer any social media or any other type of app in exchange for collecting data about you. They don't run any website where they sell ads. They trade in data – and that's all. And how they trade. Acxiom is one of the biggest actors. Even back in 2018, they had data on more than 700 million people and they have boasted that they can offer facts about everything from people's income, marital status and interests to which grocery stores they shop in and whether their boiler needs replacing.[70]

Data brokers sold information about how children moved in the physical world, which people had visited clinics linked to pregnancy and lists of people with addiction problems.

These actors track you via third-party technologies on almost every website you visit. In a way, data brokers are the ultimate proof of what the internet has become. Every time they turn up in a cookie list, they are a reminder that your online activity is being monitored. Let's use Acxiom as an example: they say they have 1500 different information points on every single one of the 200 million Americans in their system. And they haven't obtained that quantity of data simply by tracking people via cookies and other website technologies. They've amassed that quantity of data by also buying data from other actors. Data brokers buy and sell data to each other, but they also buy data from other types of tech companies; for example by buying information about your activities in different apps. In 2021, it was revealed

that data brokers had purchased location data from Life360[71], an app in which 33 million parents keep track of where their children are by tracking the child's phone. You might wonder exactly why data brokers need to know where millions of children are and who they're selling that data to. But that's just one example of how repulsive the market is. There are many more examples, particularly if we look at the type of data that data brokers sell.

In 2022, a lawsuit was brought against Kochava for having tracked hundreds of millions of people and sold sensitive data about their location.[72] The data that Kochava sold made it possible, amongst other things, to identify people who visited addiction clinics, religious institutions and safe houses for people who had suffered domestic violence. Vice reported that for a meager 160 dollars it was possible to buy a full week's list of the people who visited a specific clinic linked to pregnancy[73] – and that it's even possible to see where the visitors came from and where they went afterwards. This is data that absolutely anyone can buy. Including the state. It's emerged that authorities have purchased information about people's immigration status[74], religious belief and sexual orientation. And as early as 2013, it was possible to purchase records including addresses of police officers[75], information about people who had been raped and lists of people with drug and alcohol dependencies.

In a classic 60 Minutes interview[76], Tim Sparapani, Facebook's first Director of Public Policy, gave viewers an insight into how data brokers act and how the market works (Meta buys a large quantity of data from these data brokers)[77]. And we'll end this chapter by presenting a complete section of that conversation.

Tim Sparapani: You can buy from any number of data brokers, by malady, the lists of individuals in America who are afflicted with a particular disease or condition.

Steve Kroft: Alcoholism?

Tim Sparapani: Yes, absolutely.

Steve Kroft: Depression?

Tim Sparapani: Certainly.

Steve Kroft: Psychiatric problems?

Tim Sparapani: No question.

Steve Kroft: History of genetic problems?

Tim Sparapani: Yes. Cancer, heart disease, you name it, down to the most rare and most unexpected maladies.

Steve Kroft: Sexual orientation?

Tim Sparapani: Of course.

Steve Kroft: How do they determine that?

Tim Sparapani: Based on a series of data points they bought and sold. What clubs you may be frequenting what bars and restaurants you're making purchases at, what other products you may be buying online.

Steve Kroft: And all of this can end up in a file somewhere that's being sold maybe to a prospective employer?

Tim Sparapani: Yeah, not only can it, it is, Steve.

Steve Kroft: With all this information and your name attached to it?

Tim Sparapani: Yes. Exactly.

Ashkan Soltani (**privacy and technology specialist**)**:** The IP address and the computer ID number are recorded and it's not difficult for data brokers to match that information with other online identifiers. There are firms that specialize in doing it.

Steve Kroft: So you can combine this data with other data that's available figure out who someone is?

Ashkan Soltani: That's right.

COMMERCIAL MASS SURVEILLANCE: THE TECHNOLOGY BEHIND THE DATA COLLECTION

How the commercial mass surveillance companies collect your data and map your life.

The tech giants follow every step you take regardless of whether or not you use their services. But how does it actually work when they steal your behavior and place it in huge AI and machine learning systems to build a profile of you? Here are the methods behind the surveillance.

What techniques do the tech giants like Meta and Google use to collect data on essentially all of the world's internet users? Before we answer that question, we need to make couple of observations. 1) If you use the tech giants' services, it equates to voluntarily giving your data away. For example, if you use Facebook, Meta collects your activity there. If you use Chrome, Google registers every step you take in the web browser.[78] And no, incognito mode doesn't save you.[79] 2) You don't even need to use the tech giants' services for them to keep track of how you behave online. They reach far beyond their own user base when they collect data. Now let's take a look at how the data

is collected. And it's point 2 we'll be focusing on. Because this type of mass surveillance takes place without people being conscious of it, and without them having given their consent to it.

We'll go through the technologies used to check that it's you visiting a certain site or doing a particular search. These tools are essential for the tech giants to collect data. They have to keep track of the fact that it's you and nobody else who comes to a particular site, they have to be certain it was you that did that last Google search to add it to the right pile. Identification is the key to being able to build a profile of you. Once they know it's you out there browsing, they start up the heavy machinery: everything you do goes into huge AI and machine learning systems that register, categorize and analyze your behavior. So they can predict what you will do next, so they can try to influence you in a particular direction for commercial or political gain. Let's start with the most commonly used identification technique: your IP address.

Your IP address – the most common and simplest way of identifying you.

Everyone who has internet access has been allocated an IP address by their internet provider. This is part of the internet's basic structure. Every website you visit also has an IP address, and it's the IP addresses that make sure the traffic goes to the right place when it's sent back and forth. This is good (you want the internet to work), but it also means we each have a digital ID card that the internet service providers can use to register all the sites you visit. They are forced to carry out this logging by law in many countries. The idea is that it should be possible to reveal details about internet traffic and information about who is behind a particular IP address in case an authority asks for it (for example if the police require it during an investigation). But it doesn't stop there. Depending on what country you're in, it's

more or less likely that in practice the internet service providers give the authorities continuous access to traffic regardless of whether or not a crime has been committed. Or even sell your online behavior to make money.[80]

It's not just your internet service provider that uses your IP address to log your activity online. The IP address can be intercepted by others and used to identify, track, and map your activity. When tech giants and data brokers employ different techniques to pursue you from one site to another and map your movement patterns on the internet, one of the things they use to identify you is your IP address. The same thing applies when they study in detail what you do on each site (which texts you read, which images you stop at, which purchases you make, which products you quickly skim past, which videos you watch and so on). IP addresses can be used to link the activity and the person.

We can't be sufficiently clear here: Your IP address equates to sticking up your hand and shouting 'Here I am'. It's the easiest way to track you on the internet. And the only way to conceal your IP address, and to discard your digital ID card, is to use a trustworthy VPN (or the Tor Network). This is the reason why Mullvad was started once upon a time (in 2009, to be precise).

Third-party cookies – tracking that you accept (because you actually have no choice).

Just like IP addresses, cookies have long been part of how the internet is constructed. Cookies are on websites so the site can remember things about you – and in fact so that the site works at all. For example: you visit an e-retailer and add a product to your shopping cart. A cookie remembers the product is there when you click to go to the checkout. It's thanks to a cookie that you can stay logged into a site over time. When you choose a language on a website it's the same

thing; tiny text files (which is what cookies are) are saved locally on your computer or phone and make sure the same language is used next time you visit. Cookies make the internet a comfortable place to visit. So why is there such a fuss about cookies? Well, because there are different types of cookies.

There are cookies placed on the site by whoever owns it, so that the website is user-friendly. This type of cookie is known as a first-party cookie. They're there to give functionality to the visitor. But then there are cookies that are placed on the site for another purpose: to register your visit for somebody other than the site owner. These are called third-party cookies and they're often linked to the tech giants such as Meta and Google (or to data brokers). And because these third-party cookies are placed on the majority of websites in the world, this type of cookie makes it possible for them to monitor your movement patterns. When you hop from a news site to an e-commerce site to a streaming service, the tech giants are there every time with their cookies. And that's all they need to be able to build a single huge list of the sites you visit, and then, with the help of AI and machine learning, to build a profile of your online behavior. This type of cookie is why ads stalk you online. This type of cookie is what maps your life.

You can say No to cookies, but sometimes that doesn't even help. There are what are called 'essential cookies' that work even if you click 'Reject all'. These include cookies from the tech giants.

You can say No to cookies. Everybody who's ever been online knows that you have to click Accept, Manage or Reject cookies the first time you visit a site. The problem is that the infrastructure is constructed in such a way that you actually don't have a choice. There's widespread cookie fatigue that means we routinely click Accept to move on. Nobody can be bothered to read the almost endless user terms and conditions that appear when you click Manage cookies. And the cookie warnings are also designed for you to press Accept. The concept of dark patterns means that Accept is often a large, bold green button and that Manage cookies and Reject cookies are more or less hidden or incredibly complicated to use.

Still worse, even if you click Reject cookies, you can't be sure your visit won't be registered by a third party. There are cookies that are 'necessary'. You've undoubtedly seen the choice Accept only essential cookies. You may think 'essential cookies' are the same thing as functional cookies, but that's not true. If you click through and start to read the apparently endless terms and conditions, you often find big tech companies listed under 'essential cookies'. And in the small print, you can also see that this type of cookies can often kick in even if you choose Reject all cookies. Because the site owner has an essential collaboration with the tech giants that you don't even have the option to reject. And here's one more detail before we move on: if a website only uses functional cookies, the ones the website needs to work as it's supposed to work, you don't even need to provide a cookie warning. And so you don't even need to have the visitor click Accept. That's why you don't have to go through that process when you visit Mullvad's site.

So what can you do to prevent third-party cookies from following you wherever you go? The easiest thing is to run a web browser like Mullvad Browser, which handles that and many other things for you (cookies and IP addresses are, as you'll see if you read on, not the only

way to track you). But otherwise, all you can do is be persistent and clear out your cookies (and cache) every time you've used your web browser. You can also use many different plug-ins and extensions that block third-party cookies.

Third-party cookies have become the very symbol of how big tech and data brokers map a whole world of internet users. And the focus on this particular type of data collection has led to Google being sued for hundreds of millions of euros[240] for violating the GDPR and finally, even Google felt compelled to start looking for a way out. For several years, they worked on a new tracking system[241] that wouldn't rely on third-party cookies but on data collection via the Google web browser Chrome[242]. The launch was postponed time and time again, and eventually, Google announced that they were scrapping the initiative.

But even if Google had succeeded, the main problem would have remained. Since the issue is the data collection itself, not exactly how it is done.

Regardless of the direction in which the development is moving, it's worth remembering that third-party cookies aren't the only way for big tech and data brokers to collect data. A major problem with today's data collection is that it isn't enough to mask your IP address and make sure you block cookies. It makes no difference if third-party cookies disappear unless the business model on which the internet is now based is fundamentally rebuilt from the ground up.

As long as the collection of behavioral data is permitted, as long as it isn't illegal for companies to collect data about people and to share it with others, no change will take place – the only thing that will change is how the data is collected.

Because even if you mask your IP address and make sure you block or clear all of your cookies from time to time, there are other ways to track you via your web browser. Even if third-party cookies

are banned, this is just one of many tracking technologies. When cookies disappear as a tracking method, it's not unthinkable that what's known as browser fingerprinting will take over.

Browser fingerprinting – tracking technology that works in the shadows.

When you visit a website, the site uses technology to ask a number of questions of your web browser: this could be the version of web browser you're using, whether you're visiting on mobile or desktop, which language you have set, the time zone you're in, the different plug-ins and fonts you have installed, your screen resolution and so on. Many of the questions are also about your hardware: for example how fast your processor is and what graphics card you have installed. These are questions asked to allow the web browser to present the site in the best possible way. Just like cookies, this is part of the basic fabric of the internet that allows it to be as user-friendly as it is. But the problem is that questions are also asked that have nothing to do with functionality, but which are only there to identify and track you. The number of questions asked and the combination of answers makes it possible to take a unique fingerprint of you as a visitor.

Let's conclude by saying that in a time where third-party cookies are under legal pressure, browser fingerprinting plays by completely different rules. It's quite simply technology that you can't dismiss[81] by clicking Reject all. Because the tracking takes place completely in the shadows. And when the world begins to set restrictions on how the tech giants monitor people via cookies and IP addresses, it's not a wild guess to expect them to use fingerprinting to an even greater extent in the future.

“What makes fingerprinting a threat to online privacy? It is pretty simple. There is no need to ask for permissions to collect all this information.”

The Tor Project

Surveillance via third-party scripts – how they keep track of exactly what you do online.

Most websites use scripts (tiny fragments of JavaScript code) to work. These scripts mean that the websites work very well, but they can also be used to monitor visitors. Just like third-party cookies, this is a major problem when somebody other than the site owner is involved. If a website uses Google Analytics, there's a script on the site from Google. If a site uses a special font, there's a script from the font developer. If the site you visit uses Meta Pixel to maximize its ad revenues via Facebook, Meta has placed a script there. And when there are external scripts on the site, that's when these actors can work out exactly what you're doing.

A cookie can only identify you when you visit a site. If a cookie from the same third-party actor turns up on the next site you visit, they can start to follow you online and build a profile of how you move. The same is true with the IP address. It's a unique ID card to make sure it's you on the site. When it comes to scripts, things are a little different. They can be used to construct a browser fingerprint of you and so identify you. But above all, they can be used to take a closer look at exactly what you're doing on the site. Scripts can find out exactly which minutes of the video you watch (and not just that you're visiting YouTube again). Scripts can read how you scroll on a site, which ads you stop at and whether you've read the whole article or moved on after just half of it. It was scripts that Facebook used to collect what people had written in comment fields but then deleted and never posted.[82] Just collecting metadata – in other words the data that, together, build a profile of how you move online – is enough to map someone's life. But scripts add an extra layer.

As we mentioned above, you can block third-party scripts, and Mullvad Browser has technology to do just that. But it's important to remember that if a data collector succeeds in recording exactly what

you're doing on a site via scripts, they still need to identify that it's you visiting for it to have any effect. If you mask your IP address using a trustworthy VPN and use a web browser that makes sure it's hard to identify you via cookies and fingerprints, it doesn't matter how accurately they can measure which parts of a YouTube video you most enjoyed – they still don't know that it's you.

Sophisticated AI comes with new kind of threats. The mass surveillance of tomorrow will be something else, and we need to work on resistance today.

Sophisticated AI technology poses new threats.

Using a trustworthy VPN and a privacy-focused browser is an easy way to counteract the data collection that takes place through the methods we have mentioned in this text. But you should remember that things are developing quickly and that those interested in mass surveillance are constantly working on new technologies. One growing threat is traffic analysis.

When you visit a website, network packets are exchanged. These data packets are sent back and forth between you and the websites you visit. This is how the internet is fundamentally constructed. And the fact that the packet is sent, how often they are sent, and the actual size of those packets – all this is something that's visible to your ISP, whether or not you're using a VPN (or Tor).

Every website generates a specific pattern of data packets that are sent back and forth (depending on how the site is constructed with images, text blocks, and videos), which means that your internet service provider (or anyone who has access to your internet service provider) can look at this pattern of data packets and try to analyze it to work out what websites you visit, but also to find out who you are communicating with by using what's known as a correlation attack (you sending a message with a special pattern at a given time and someone receiving that particular traffic pattern at the same time).

These are advanced attacks, but given the speed with which artificial technology is evolving, and its ability to analyze large amounts of data, it's a growing threat.

In response, Mullvad has developed DAITA (Defense against AI-guided Traffic Analysis), which, as the name implies, is a defense against this type of traffic analysis using AI. We have worked with Karlstad University to develop a technology that can be turned on in our VPN app and which makes sure the data packets sent are always the same size – and also sends out fake packets.

We have also worked with researchers to develop VPN tunnels that can withstand the quantum computers of the future, which potentially could be able to crack encryption.

We don't know how this type of technology will be used for mass surveillance of entire populations in the future, and so we must work on countermeasures today.


WAIT A SEC! AT LEAST WE CAN SEE WHEN COMMUNICATION TAKES PLACE, AND THE AMOUNT OF DATA SENT. IF WE LET AI ANALYZE IT, THEN MAYBE WE CAN MAP...
CRAP! MULLVAD IS NOW MIXING IN FAKE DATA TO THE NETWORK TRAFFIC. GOOD LUCK FINDING PATTERNS IN THAT MESS.
ENCRYPTED COMMUNICATION
DATA TRAFFIC
DATA BROKERS
MAX 2024

COMMERCIAL MASS SURVEILLANCE: THE COLLECTED DATA CAN'T BE KEPT ANONYMOUS

Organizations that collect data often claim it's anonymous. Research shows this is impossible.

When the tech giants collect huge quantities of data about your internet behavior, they always hide behind defenses such as 'it's only metadata' or 'we've anonymized the information'. But if you collect big data, it's impossible to keep it anonymous. It's enough for your phone to reveal four places you've been to work out that it's you.

When tech giants collect data about people, they have two standard excuses. The first one is: 'It's only metadata'. In other words, they're saying it's not a problem because they don't collect the actual conversation between two people (although in fact they do) or anything else concrete (in their eyes). But as we've already explained, metadata equates to mapping someone's life. After this, they usually say: 'We've anonymized the data'. And then they talk about how they've replaced the digits in an IP address or simply hidden it. Or removed other information that can be linked to a particular person. But the fact is that if you collect sufficient data, it's impossible to keep it anonymous.

And because the entire business model of the tech giants is based on big data, this means your internet behavior can undoubtedly be linked to you as a person. For example, if you have access to several different databases and can compare them, you can de-anonymize people very quickly. Like when Netflix released 10 million film ratings from half a million anonymous users and, to prove the point, a team of researchers at the University of Texas[83] succeeded in identifying several of them simply by comparing the ratings and the time they were made with ratings published publicly on the IMDb. And here's another example: when the State of Washington sold medical data about anonymous patients for 50 dollars a time[84], Harvard researchers could put names to several of them by comparing parts of the records with news articles about accidents and violent crimes.

It's difficult to identify someone if you only have access to one or two data points. But as soon as you have access to more, you can use classic exclusion methods to work out who's behind the information. In his book Data and Goliath, cryptographer and security expert Bruce Schneier gives a good example: The FBI needed to track someone sending anonymous emails from different IP addresses. When they looked at the IP addresses, it turned out they all belonged to different hotels. The person had been careful to change the hotel every time they wanted to send an email. But all the FBI had to do was examine the customer records from the different hotels. Was there somebody who'd checked in at all the hotels when the emails were sent? They didn't have to look at many hotel stays before the list came down to a single person.

Research has often shown that you don't need many data points to identify people. The fastest way is by using location data, if you have access to several places an anonymous person has visited. Think about it: there may be hundreds of people at your workplace, but how many of them shop in the same grocery store as you? There are

perhaps a couple of you that match both of these points. But add a few more data points and you're done. Researchers at universities in the UK and Belgium have published methods saying that it's possible to identify 99.98% of people on anonymous lists[85] if there are a mere 15 demographic attributes. Another group of researchers say that you only need four data points – if they contain place and time – to identify 95%[86] of individuals. In a further study, researchers looked at three months' credit card statements[87] to determine that it was sufficient to have four points – once again regarding place and time – to identify nine out of ten people.

The researchers had access to search histories from 657,000 users. There were no names, only a number linked to each list of searches. When they were done, they'd replaced the numbers with names.

Given how much data is collected about each of us as soon as we start up a web browser, anyone who wants to use the data (and de-anonymize it) barely needs to even use place and time parameters. Amongst the examples Bruce Schneier gives is when researchers examined the search history of 657,000 users. In total it involved 20 million searches and the information was, as they say, anonymized. There was only a number linked to each list of searches. But by correlating different pieces of data, the researchers could replace numbers with names. We'll say it again: your internet behavior is tracked and logged in detail. It doesn't take long using exclusion methods to reduce the options down to just you.

STATE MASS SURVEILLANCE

Democratic and authoritarian countries are competing to see which of them can carry out mass surveillance most and best (worst).

USA and their friends in the surveillance alliance Fourteen Eyes have demonstrated that they have the capacity, the desire and the experience to monitor who they want, when they want, anywhere in the world. China and other totalitarian countries use mass surveillance to control their inhabitants. It often feels like a dystopian arms race is going on around the world. But who is actually the best (worst) at making George Orwell's 1984 a reality?

There are two types of mass surveillance. Commercial, which you have already read about. And mass surveillance carried out by states and rulers. Both are reprehensible, and our attitude is well-established: mass surveillance infringes individuals' human rights[88], invades the personal privacy free societies are built on, and is also ineffective against the problems it's claimed to solve. This is the ultimate core of our business. Our company was founded in 2009 because the surveillance laws were going in the wrong direction, and our message

to those in power all over the world is the same now as it was then: there's a difference between surveillance and mass surveillance. Don't get involved with the latter: don't carry out mass surveillance on your population or that of other countries. Use targeted surveillance if there's a suspicion of a crime, in a proportional way and via independent court decisions.

We think human rights are worth preserving and defending. And it's important to remember that they're there to protect people against the state. They are a landmark to cling to, to prevent the worst parts of human history repeating themselves. They are there because people and those in power take bad decisions. Because governments change. Because no state should have total and uncontrollable power. Ultimately, the state should be there for the people and not the other way round.

Even if a large part of today's mass surveillance is global, it originates in different countries and changes depending on what country you live in. So, let's take a look at some of the clearest examples of how widespread it has become in large parts of the world.

USA – with the capacity and experience of monitoring the entire population of the world.

There's a problem with reporting the mass surveillance carried out by countries like the USA (at least if you want to stick to proven facts): they aren't very happy about you talking about it. Of course there are exceptions. Like when self-satisfied managers like the CIA's chief technology officer Ira 'Gus' Hunt give presentations and boast to journalists about how "we try to collect everything and hang onto it forever".[89] Or when a senior Defense Department official explains that not even the Pentagon's employees can expect to have their privacy respected: "We want our people to understand: they should make no assumptions about anonymity. You are not anonymous on this planet

at this point in our existence. Everyone is trackable, traceable, discoverable to some degree".

And sometimes a building says more than a thousand words, like when the NSA constructs enormous server halls out in the Utah desert to store data.[90]

But to get mass surveillance down in black-and-white, to produce hard facts and figures, it requires brave whistleblowers like Edward Snowden. It's only through this type of hero that we get an insight into what's actually going on. Even now we still don't have better answers than what Snowden gave us in 2013. We'd hoped for change in the wake of his revelations, but unfortunately they're still relevant today, so that's where we'll start.

Snowden's revelations showed that American authorities were monitoring hundreds of millions of people all over the world – every day.

American mass surveillance is possible thanks to Section 702 of the Foreign Intelligence Surveillance Act (FISA)[91], a law that the USA renews every five years. Section 702 is the key to why American authorities need no court decisions to monitor people. The law came into being on the pretext that terrorists were being tracked after the 9/11 attacks, and would 'only' refer to eavesdropping on non-American citizens, but as the law is written and as the internet is constructed, in practice it means surveillance of both foreign and American citizens. When Snowden's revelations emerged, it also turned out that it wasn't just being used against people suspected of a crime, but that the American administration was carrying out mass surveillance of

millions of people.[92] Other documents that Snowden leaked demonstrated how the National Security Agency (NSA) had the capacity to monitor essentially every person on the planet, and that they weren't saving their powder: the documents showed, amongst other things that they collected 200 million text messages from different parts of the world – every day.[93]

Using the program Xkeyscore, the NSA's analysts had access to a database covering "nearly everything a typical user does on the internet".[94] This included both direct data like emails in people's inboxes, chat conversations and private messages on Facebook. But also things categorized as metadata; search histories and exactly what sites millions of people were visiting. Using XKeyscore the analysts could also do searches on people's internet behavior – entirely without judgments from either a court or even a superior inside the NSA.[95] Either via a hard search: for example through an IP address or email address, which could give them access to virtually everything a specific person did online. Or via a soft search: a search for a keyword or phrase, which could give them lists of people with a particular internet behavior. Snowden showed the world how easy it was for the NSA to search in XKeyscore and how much they could get out from the program. But where did all the data come from?

Section 702 contains two parts that give American authorities such as the FBI, CIA and NSA access to enormous quantities of data, and they go by the names of Prism (downstream) and Upstream.[96]

Prism means that they have the right to demand data from American companies without a court decision. When the authorities have free rein to request information from the world's biggest tech companies, it's not surprising that it ends in mass surveillance. But Snowden revealed that the situation was even worse. The leaked documents revealed that the authorities didn't even need to request the material, but that they more or less had direct access to the tech

companies' systems and servers.[97] As Snowden wrote in his book Permanent Record: "Prism enabled the NSA to routinely collect data from Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, Skype, AOL, and Apple, including email, photos, video and audio chats, Web-browsing content, search engine queries, and all other data stored on their clouds."

Of course all the tech companies on the list denied that the FBI, CIA and NSA had direct access to systems and servers. Which maybe wasn't all that strange, because the law can actually mean that it's illegal for the companies to admit their involvement.[98]

"The systems reacted to keywords such as 'anonymous internet proxy' or 'protest'. There, algorithms decide which of the agency's exploits – malware programs – to use against you. Once the exploits are on your computer, the NSA can access not just your metadata, but your data as well. Your entire digital life now belongs to them."

Edward Snowden

While Prism gave the NSA the right to demand data from American companies such as Microsoft, Facebook and Google, Upstream[99] gave them the right to directly connect to the backbone used by American telephone and internet service providers. This involved major American telecoms companies such as AT&T[100] but also the world's biggest router manufacturers, who built monitoring for the NSA into their products.[101] Snowden again:

"Upstream collection, meanwhile, was arguably even more invasive. It enabled the routine capturing of data directly from private-sector internet infrastructure – the switches and routers that shunt internet traffic worldwide, via the satellites in orbit and the high-capacity fiber-optic cables that run under the ocean."

It would take a lot to prevent global internet traffic from traveling via American servers, cables and services. That's how the digital infrastructure and power relationships are constructed. In principle, Prism and Upstream therefore gave the American authorities the possibility of monitoring every person on the globe. Snowden showed that they could search people's history, but also monitor them in real time. Handling that quantity of data required sorting, which was done via the Turmoil and Turbine programs. In Permanent Record, Snowden wrote:

"You can think of Turmoil as a guard positioned at an invisible firewall through which internet traffic must pass. Seeing your request, it checks its metadata for selectors, or criteria, that mark it as deserving of more scrutiny. Those selectors can be whatever the NSA chooses, whatever the NSA finds suspicious: a particular email address, credit card, or phone number; the geographic origin or destination of your Internet activity; or just certain keywords such as 'anonymous internet proxy' or 'protest'. If Turmoil flags your traffic as suspicious, it tips it over to Turbine, which diverts your request to the NSA's servers. There, algorithms decide which of the agency's exploits

– malware programs – to use against you. Once the exploits are on your computer, the NSA can access not just your metadata, but your data as well. Your entire digital life now belongs to them."

Snowdens whistleblowing revealed that the American authorities were eavesdropping on people's conversations, reading their messages and even looking right into their homes via cameras in computers and mobile phones. And yet it's common for states carrying out mass surveillance to deny it and try to hide behind the phrase 'we only collect metadata'. As if that wasn't enough. American cryptographer and security expert Bruce Schneier describes it as follows in his book Data and Goliath:

"In a text message system, the messages themselves are data, but the accounts that sent and received the message, and the date and time of the message, are all metadata. An e-mail system is similar: the text of the e-mail is data, but the sender, receiver, routing data, and message size are all metadata. Metadata may sound uninteresting, but it's anything but. Collecting metadata on people means putting them under surveillance. Eavesdropping gets you the conversations. Surveillance gets you everything else. Metadata reveals our intimate friends, business associations. It reveals what and who we're interested in and what's important for us, no matter how private."

Metadata includes all the websites you visit and your entire search history, and when you realize that, the 'we only collect metadata' defense suddenly becomes very thin. Stewart Baker, former general counsel for the NSA, expressed this clearly[102]: "Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."

For example, metadata can be used to identify journalists critical of the American mass surveillance apparatus. Two of them are Laura Poitras[103] and Glenn Greenwald[104], the journalists Snowden reached out to when he decided to blow the whistle. Snowden chose

them because they had already criticized the NSA and had suffered personal consequences as a result. When he handed over the documents to them, in that Hong Kong hotel room, it was revealed that the NSA partner GCHQ had been monitoring journalists from the New York Times, Le Monde, and the Washington Post, among others, and classified investigative journalists as a threat equal to terrorists and hackers.

The fact that the NSA was monitoring journalists wasn't particularly surprising. The American surveillance apparatus wasn't merely eavesdropping on terrorists and criminals. They were also carrying out industrial espionage[105] and monitoring human rights organizations like Amnesty and Human Rights Watch.[106] They weren't simply listening to hundreds of millions of Americans, but for example also captured 70 million French phone calls per month.[107] And of course the system was used to monitor politicians and world leaders.[108]

We haven't been able to get as good an insight into how the American authorities work since Snowden's revelations. We don't know exactly how they carry out mass surveillance today. But Section 702 has been extended. And every year since 2013, more and more information has emerged about how the NSA, CIA and FBI are sticking to their tactics of not merely monitoring suspects, but carrying out mass surveillance of the entire population.[109]

In 2017, we all got a new insight into the American mass surveillance apparatus. The leak was far from as comprehensive as Edward Snowden's, but it was clear that these activities were still continuing when Wikileaks revealed that the CIA had hacked into people's phones, computers and TVs[110] to carry out mass surveillance. And this time, not even the commercial partners denied it[111]: "If your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition", as Samsung expressed it.

“End-to-end-encryption was a pipe dream in 2013. An enormous fraction of global internet traffic traveled electronically naked. Now, it is a rare sight. But the capabilities governments had in 2013 seem like child’s play compared to today.”

Edward Snowden

The quote could have come directly from George Orwell's 1984 dystopia, with its telescreens that both sent out propaganda and listened to the population.

In 2023, Snowden gave his picture of how the world had changed, ten years after he had become a whistleblower.[112] He spoke about how his revelations had made the tech companies introduce end-to-end encryption and that in many ways it's no longer as easy for authorities to simply eavesdrop on all internet communication. At the same time, the technical skill and development have advanced enormously, even on the other side. As Snowden expressed it:

"If we think about what we saw in 2013 and the capabilities of governments today, 2013 seems like child's play. The idea that after the revelations in 2013 there would be rainbows and unicorns the next day is not realistic. It is an ongoing process. And we will have to be working at it for the rest of our lives and our children's lives and beyond."

The tenth anniversary of Snowden's revelations received widespread attention, and the majority of sources were in agreement that global mass surveillance has certainly not ceased, merely found different approaches.[113]

It has emerged that organizations including the FBI and other three-letter agencies have purchased collected data from data brokers[223]. But why do American agencies, who already have an exemption allowing them to monitor people without a court order, buy data from data brokers? Well, for a start, when they buy data, they needn't claim that American citizens "happened to be caught up in surveillance of foreign threats". It's likely also true that commercial data collection has become so widespread and so invasive that it's cheaper and more convenient for the agencies to simply purchase the data rather than doing the job themselves. As one consultant for the American government put it, in an article about how the American agencies used data collection via apps to track some of Putin's closest

entourage[224]: "The advertising technology ecosystem is the largest information-gathering enterprise ever conceived by man."

Or as Michael Morell, former director of the CIA, put it[225]:

"The information that is available commercially would kind of knock your socks off. If we collected it using traditional intelligence methods, it would be top secret-sensitive. And you wouldn't put it in a database, you'd keep it in a safe."

The reason why the CIA had been forced to keep it secret, if they had collected it themselves, is obvious – the agency isn't permitted to carry out this type of data collection according to the American Constitution (although they still do it anyway via the Section 702 exemption to the Foreign Intelligence Surveillance Act).

In recent years, the fact that American agencies have purchased large quantities of data from data brokers has contributed to an increasingly heated discussion about Section 702 – the law that the Americans extend every five years which makes it possible for their agencies to carry out mass surveillance without a court order. Senator Ron Wyden has been one of the most voluble critics and has urged the government[226] that it "should not be funding and legitimizing a shady industry whose flagrant violations of Americans' privacy are not just unethical but also illegal."

The debate became a hot topic in 2023 when it was once again time to renew Section 702 for a further five years. The House of Representatives failed to pass the extension bill on three occasions and was forced to delay the decision until spring 2024. At the same time, amendments to the law were suggested[227]. The biggest proposed amendment would force agencies to have court approval before they were able to monitor American citizens. Another proposal would prevent the NSA from carrying out 'abouts collection' – in other words monitoring aimed not just at people communicating with surveillance targets, but also involving communications where the target has merely been mentioned.

In other words, a minor storm erupted about the latest extension of Section 702, indicating deeper awareness of and broader skepticism to American mass surveillance. But how did it end? Well ultimately both the House of Representatives and the Senate still voted an extension through – but following the debate in the House of Representatives, the extension will only run for two years instead of the normal five. This shorter extension could have been seen as a step in the right direction if it wasn't for the fact that an expansion of the law was also voted through at the same time. Because despite all the protests and debates in the House of Representatives, when the extension was passed the majority in both the House of Representatives and the Senate had no problem expanding the list of companies that, according to the law, can be forced to collaborate with government agencies and their mass surveillance of the population[228]. The definition of organizations that must permit surveillance is now so broadly described that it could even include anyone with physical access to a target's communications infrastructure, such as routers[229]. Senator Ron Wyden called the expansion "dramatic and terrifying."[230] Edward Snowden commented on the issue by stating: The NSA is taking over the internet."[231] Instead of a step in the right direction, the exemption became more invasive than ever.

Europe – countries in close collaboration with the USA. Sometimes even worse than Big Brother.

But Edward Snowden's whistleblowing didn't expose only the actions of the American authorities. In the same way as the US Upstream system, the UK connects directly to the fiber optic network between the USA and Europe, and gives what it calls the Tempora program[114] access to internet traffic between the two continents. With Tempora, the British intelligence organization GCHQ could, it claimed, "Master the internet", and Snowden's leak showed that it was a very apt

description. In 2013, 300 GCHQ and 250 NSA employees worked full time to analyze the data that arrived via 40,000 different key triggers.[115] In total, 850,000 NSA employees had access to the British system[116], which processed 600 million 'telephone events' and other traffic every day via 200 fiber cables. Snowden called Tempora "the largest program of suspicionless surveillance in human history".[117] But what did GCHQ have to say? When they trained new analysts in the tool, the presentation had the title "You are in an enviable position – have fun and make the most of it". It suddenly doesn't sound so unlikely that NSA employees would pass around naked pictures of the people they were monitoring.[118]

And the USA and UK aren't the only countries collaborating and sharing surveillance between them. Since the Second World War, the countries in the Five Eyes electronic eavesdropping alliance have shared data amongst themselves. From the outset, the members of the English-speaking Five Eyes pact were Australia, Canada, New Zealand, the UK and the USA. But Edward Snowden's leaks revealed that the alliance had been expanded and that it now went by the name Fourteen Eyes, with the new members being Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain and Sweden.

VPN actors who claim they are better because their business isn't in a Fourteen Eyes country are ignorant and dishonest. The internet is a global phenomenon, and your traffic crosses the borders of several Fourteen Eyes countries as soon as you start to surf, regardless of where your VPN company is based.

It's important to emphasize: Mullvad VPN is a Swedish company, and our business is based in a Fourteen Eyes country. That has absolutely no impact on our users. The Fourteen Eyes agreement is based on collaboration between intelligence services and on the fact that they sometimes share the internet traffic that crosses their country borders in the physical cables that, for example, run under the Atlantic. As we've already observed, the internet is a global phenomenon and the majority of traffic is sooner or later routed via the USA, so it's really not important where a VPN actor is based. Regardless of where their business is in the world, and regardless of where their servers are, their users will not be able to remain within those borders, because they will naturally visit websites and use services that are located elsewhere. In addition, these 14 countries were revealed more than 10 years ago. No VPN actor knows how high the figure is today and which countries are involved.

But fortunately, the whole idea of a VPN is to encrypt traffic, to make it impossible to read, for example if an authority has connected to a fiber cable. So when VPN actors claim they are better because their business is based 'outside Fourteen Eyes countries', it's not only proof of a serious lack of knowledge, it's also dishonest and misleading. When it comes to where your VPN actor is based, only the country's laws are relevant. The laws that control how a VPN service must log and reveal data are crucial. Sweden is a good country from this perspective.

It's hardly news that the intelligence services in different countries collaborate, and nor is it a problem. The problem is that they do so via mass surveillance, despite the fact that it's constantly being judged as horrifying and illegal. In 2018, the European Court of Human Rights stated that the Tempora program was illegal and incompatible with the conditions required for a democratic society[119] and in 2020, an American court decided that the NSA surveillance of hundreds of millions of people was unlawful and unconstitutional.[120]

You might be forgiven for thinking that such repeated scandals would tip the world in another direction. But instead, it seems like mass surveillance is simply getting more and more extensive.

An intense tug-of-war is under way in the EU. At one end: the EU's highest court, which over and over again rules that mass surveillance[121] is illegal, plus the part of the EU trying to put legal pressure on tech companies via directives such as the GDPR. Up to now, the GDPR Directive has been largely ineffective, and has mostly succeeded in handing out symbolic (in the context) fines to the world's richest companies while simultaneously making the internet experience a cookie nightmare for every user. But this type of regulation has actually started to put pressure on big tech companies like Meta and Google.[122] Hopefully this will ultimately lead to something good, but there's a risk that the tech companies will simply adapt, regroup and come up with new solutions to collect data. But we still applaud attempts from the EU and hope that this is the power in Brussels that gets the longest straw. Because there's another side in this battle, that's pulling in completely the opposite direction.

At the other end of the rope, for example, we find EU countries like France, which wants to introduce AI video surveillance[123] and a Hungary installing black boxes allowing the state direct access to ISPs' networks[124], and therefore to users' internet behavior, without a court decision.

In the same sphere, we also find parts of the commission wanting to introduce a total prohibition on private communication with its proposed chat control law[125], which would mean mass surveillance on a level that would even make the NSA jealous. Needless to say, we're closely following the battle between those who want to transform the EU into an authoritarian alliance and those who actually care about privacy and are attempting to provide a good example for the rest of the world.

In the UK too, there are powers that want to undermine the encrypted traffic that's become more popular since the Snowden revelations, through the draft Online Safety Bill.[126] In both Europe and other parts of the world, we've also seen how Pegasus spyware is used by countries to target dissenters, political activists and journalists.[127]

Governments and authorities in democratic countries have shown that they have no problem carrying out mass surveillance of entire populations and looking straight into law-abiding people's homes via phone cameras and microphones, TVs and computers. And their authoritarianism shines through their ambitions, like when EU Commissioner Ylva Johansson thinks the EU's experts and independent regulatory authorities make it difficult for Europol to do its work.[128] It bears repeating: human rights are there to protect people against the state. And it's also important to remember that rights are something you also have to fight for.

Authoritarian countries – don't conceal their ambitions for their mass surveillance.

The fact that totalitarian countries also use mass surveillance scarcely needs saying. In the world, there are more than 4.5 billion internet users. 76% of them live in countries that imprison people for things they've written online about political, social or religious issues.[129] Almost as many live in countries that block and censor online content. In other words, in authoritarian countries a VPN isn't used only to reduce mass surveillance, but also as a tool to even be able to get out into a free, uncensored internet, so that people can gain free access to information.

Here are a couple of examples: in Iran, the state has become known for switching between completely shutting down the internet and allowing its surveillance program, SIAM, to control, filter and monitor how people use their phones (via the mobile network).[130]

In Egypt the government monitors journalists, activists, and lawyers[221]. In Morocco the authorities have used Pegasus to monitor[222] human rights organizations.

In Russia, the Russian Federation's federal security service (FSB) has long used the SORM system to eavesdrop on phone calls, and to read emails and messages.[132] By combining this with censorship, blacklisted technology and other surveillance, Russia's really cracking down hard on its citizens. In Moscow, the state has introduced a system that combines several hundred thousand surveillance cameras, facial recognition and monitoring of mobile data.[133] The system has been used to track and imprison demonstrators, political opponents and journalists. They call both the program and the Moscow's digital infrastructure 'Safe City'.

Ironically, however, this massive mass surveillance system has begun to bite the hand that feeds it. On the digital black-market cyber bazaar known as Probiv[134], corrupt and/or poorly paid and dissatisfied officials have begun leaking data from the enormous databases resulting from mass surveillance. The problem for those in power in Russia is that they're in the database too. For a very small sum, it became suddenly possible to buy information about Putin's innermost circle[135], which the opposition, other countries and investigative journalists didn't hesitate to exploit.

The Great Firewall of China controls and censors the internet for 750 million inhabitants. They are under total surveillance and the police system claims to be able to predict when someone is going to commit a crime, and where.

The list of countries using mass surveillance[136], censorship and persecution on their citizens is a long one. At freedomhouse.org there's a good review of the situation in different countries[137] and how the trends look (spoiler: the world has declined by this measure 12 years in a row). Many countries compete to be worst in the world, but regardless of how you count it's very difficult not to think that China beats them all.

The Chinese state controls the country's 750 million internet users in an "utterly mind-boggling way", as Edward Snowden has put it.[138] The state controls the sites users can access, blocks VPN services and requires inhabitants to register using their real name to be able to post content.[139] Social media and messaging apps in the country are under state surveillance[140], foreign apps are prohibited and even TikTok, which was founded in China, has a special version that blocks international content.[141] Internet service providers in the country are forced to collaborate with the state, and all of China's mobile phones are under constant monitoring via location data.[142] The Chinese people's internet experience is completely controlled and censored under what's known as The Great Firewall of China[143] and even by 2013 there were 2 million 'internet public opinion analysts'[144] working manually to censor citizens' messages online.

But of course the country doesn't work merely with manual monitoring. In what has been called 'public opinion analysis software'[145], the state collects data and uses AI to react to 'sensitive material'. The list of activists, journalists and perfectly ordinary people imprisoned for criticizing China online seems endless.[146] You only have to insult 'heroes and martyrs' to risk spending three years behind bars.

In the Police Cloud[147], the state has also constructed a system based on big data which is said to be able to 'visualize' hidden trends and relationships between people. Using this system, the state draws up relationship maps and registers what it calls 'extreme opinions'.

Another part of the program is claimed to be able to predict crime and where it's most likely to take place.

China also collect 'voice prints' from people[148], has installed more than half of the world's 1 million surveillance cameras[149] and has also introduced technology that not only contains face recognition but can even identify how you're feeling.[150] Overall, the image emerges of a surveillance society that's not merely reminiscent of the dystopian societies we've read about in science fiction but in many ways goes well beyond them.

The documentary Total Trust[236] describes how the Chinese Communist Party "solves problems at grassroots level" by allowing 4.5 million 'grid officers' to maintain records on how the inhabitants of different areas (grids) behave. If somebody is suspected of doing something 'unsuitable' they quickly receive a visit from the police.

To help them, they have the 'Sharp Eyes' project, which takes the form of a large number of surveillance cameras used by the government to keep track of citizens, but which so-called 'volunteers' can also use to denounce their neighbors. "The People have sharp eyes," as the government puts it.

Through the hundreds of millions of surveillance cameras, biometric AI and total monitoring of people's online behavior, they have managed to connect the digital world to the physical.

Together the many millions of surveillance cameras in the country create what they call 'Skynet.' The cameras are located not only out on

the streets and outside the homes of those who have been classified as 'unsuitable', but also inside stairwells and at the front doors of those always ready to inform on their neighbors.

Through the hundreds of millions of surveillance cameras, biometric AI (such as facial recognition, eye recognition, and voice recognition) and total monitoring of people's online behavior, they have managed to connect the digital world to the physical. When people who refuse to stand for the regime's injustices get ready to leave their homes to meet a lawyer, complain about a government agency, or for any similar activist activity, the police already know about it and put staff in stairwells to carry out temporary house arrests.

But temporary house arrest or police custody is far from the worst that can happen. In 2015, hundreds of human rights lawyers were imprisoned and tortured in what is known as The 709 Crackdown[237]. Those not imprisoned are monitored constantly. Journalists who have written about their experiences have had their phones tapped and have been imprisoned[238].

How does the Chinese government justify all this? By saying that they are creating safe communities and smart cities[239].

For authoritarian countries, mass surveillance is a tool of control, and significant resistance will be needed to improve the situation for the inhabitants of those countries. In totalitarian states, the technologies used to persecute dissenters, censor information and stifle protest movements. There's no doubt about this – and this type of country isn't exactly ashamed of it, either.

Democratic countries don't boast about it as much and the consequences for those affected are not as severe. But we've already seen how mass surveillance is used to win free elections and how dissenters and journalists are monitored. There are several democratic countries on a slippery slope and the question is where they will end up when history is being written. Do they want to continue being

democratic or not? Because that's what mass surveillance is about. Mass surveillance equals control and is the opposite of freedom. And there's a boundary somewhere. Somewhere, you finally lose your position as a free society. That's why we fight for a free internet. Free from mass surveillance, data collection and censorship.

Where will the democratic countries end up when history is being written? Do they want to continue being democratic or not? Because that's what mass surveillance is about. Mass surveillance equals control and is the opposite of freedom.

STATE MASS SURVEILLANCE: GOING DARK

Going Dark: The war on encryption is on the rise. Through a shady collaboration between the US and the EU.

Under the slogan 'Think of the children', the European Commission tried to introduce total surveillance of all EU citizens. When the scandal was revealed, it turned out that American tech companies and security services had been involved in the bill, generally known as 'Chat Control' – and that the whole thing had been directed by completely different interests. Now comes the next attempt. New battering rams have been brought out with the 'Going Dark' initiative. But the ambition is the same: to install state spyware on every European cell phone and computer.

On May 11, 2022, EU Commissioner Ylva Johansson presented a legislative proposal under the official name "Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse."

Ylva Johansson made a point of this being her bill: it was she who had devised it – no one else – and if it had not been for her, Europe's

justice system would "go blind" in the hunt to track sexual abuse of children. In Ylva's world, the EU would "turn into a pedophiles' paradise" if she didn't get her way. It was easy to marvel at how, on almost every occasion, Ylva Johansson was keen to point out that this was her proposal. A touch of narcissism? Maybe. But perhaps there was something else behind this self-centered proclamation. Because it would eventually emerge that in fact Ylva Johansson was not alone behind the scenes. Right from the start, there were others involved – actors who would benefit from the bill being passed, but who preferred it not to be known that they were involved in designing it.

The rhetoric was clear from day one: it was all about the children, and when it comes to children, there's nothing we can't imagine doing to keep them safe. So Ylva Johansson put forward a proposal that meant total surveillance of all EU citizens and as soon as someone opposed it, she pulled out the think-of-the-children card. But those who could see through the bluff quickly gave the proposal (those parts of the bill that dealt with internet surveillance) a shorter and more appropriate name: Chat Control.

When Ylva Johansson was asked whether it would be possible to communicate safely even after her bill was introduced, she answered "Yes." And a whole world of experts asked "How?" Ylva replied that she had something nobody else had. A digital sniffer dog.

In brief, Chat Control essentially meant that the communications of every EU citizen would be monitored. Every call, every message and

every chat, all the emails, photos, and videos saved in cloud services – all of it would be filtered in real time via artificial intelligence and then checked in a newly established EU center, in close cooperation with Europol.

Since the bill was in violation of the European Convention on Human Rights, the EU Charter and the UN Declaration of Human Rights, Chat Control was rejected by one legislative body after another. Both the Council of Ministers and the European Commission's own legal service[244] warned against the proposal, as did the European Parliament's Data Protection Board[245]. The UN Human Rights Council described Chat Control as incompatible with fundamental human rights and stated that the proposal would lead to mass surveillance and self-censorship[246]. Former judges at the European Court of Justice said that the proposal was in breach of the EU Charter of Rights[247] and 465 researchers joined forces to warn of the consequences[248].

Faced with massive criticism, Ylva Johansson defended herself. According to her, everyone else had misunderstood the bill. Chat Control was certainly not about mass surveillance and everyone making that claim was simply out to discredit her.

Chat Control – total monitoring of all EU citizens.

Chat Control is sometimes also called Chat Control 2.0, since existing legislation already makes it possible for tech companies such as Google and Meta to scan their users' accounts for child pornography material. The fact that there was already a law that allowed tech companies to scan for illegal content – if they chose to – was something Ylva Johansson was not slow to mention. She explained that her draft bill was nothing but an extension of the scanning that had already been going on for ten years[249]. She also referred to the existing legislation when she said that the EU would become a free zone for

pedophiles unless her bill went through – as that legislation would expire in the summer of 2024.

Time and time again Ylva Johansson was proven wrong by journalists and experts. In fact, nothing prevented the EU from extending the existing law, rather than introducing a new one. And above all: Ylva's bill was anything but an extension. The differences between the current law and the proposed legislation were extreme. In Ylva Johansson's EU, scanning would not be voluntary. All messaging services (including encrypted services such as Signal) would be covered by the law and would be forced to scan their users' images, videos and conversations. That would be a big concern for all those who don't use Meta or Google to converse because they are in need of secure communication methods. In other words, political opponents, whistleblowers, journalists and their sources, vulnerable people living under secret identities and others, not to mention people with trade secrets, and those in possession of sensitive information important for national security. For example, the European Commission itself uses Signal. Demanding government transparency (either through so-called backdoors or scanning on the computer or phone) would open a Pandora's box to countries with authoritarian inclinations (five EU countries have already been caught[250] using spyware to monitor political opponents) and would leave the door wide open for criminals to exploit. But it was not only this that separated the existing legislation from the draft bill that the European Commission wanted to introduce.

The previous legislation had only allowed scanning for material that had previously been stamped and registered as child pornography material. Now, AI would be used to find 'new material' and would also look for grooming attempts. Quite obviously, Chat Control would therefore send every other citizen of the EU straight into the filtering system. Holiday photos from the beach, nude photos sent between

partners, dirty text messages – all the things that no AI system can distinguish between would risk getting caught in a filter that would inevitably drown any new EU center with endless digital heaps of evidence to review. Is this a holiday photo of a child or child pornography? Are these skimpily dressed youngsters 18 or 14? Is this a dirty text message from a wife to a husband or a grooming attempt? But above all, Chat Control would mean a tool that could be used to scan for completely different things.

When Ylva Johansson was asked whether it would be possible to communicate safely even after her bill was introduced, she answered "Yes." And a whole world of experts asked "How?" Ylva replied that

she had something nobody else had. A digital sniffer dog that could smell encrypted communication without looking at the content. A sniffer dog that only reacted to child pornography content – never anything else.

Ylva Johansson was employing blatant deception. She used incorrect figures and biased surveys. In interviews, she was populist and evasive.

A group of experts tried to hammer the message home: either encrypted communication is encrypted (so-called end-to-end encryption, which only the sender and the recipient can see) or it's not encrypted. There's no 'seeing the content' without reading it. But Ylva stood by her claim. She came back to the same argument over and over again. She avoided answering the questions (she obviously didn't understand how the technology worked) but instead turned the direction of the discussion, saying, for example, that a court order would be required to carry out scanning, which in itself was deliberately misleading. Firstly, her scanning would not require an order from a court – it could be one from another judicial body. And secondly, the key issue was that judicial body making a decision that would force messaging services to monitor all their users. So in other words, when Ylva proclaimed "it requires a court order," she wasn't talking about courts and their decisions to monitor people such as suspected pedophiles. She was talking about how a service would be forced to permit surveillance. What was required for a service to be subject to surveillance? Merely that there was a possibility to use the service to spread child pornography or to groom children. Which of course means every messaging service on the planet.

As soon as Ylva Johansson was shown to be in the wrong, she shifted her focus. But in the end, she always came back to the final refuge: it's all about the children. She related anecdotes and referred to figures that pointed to an exponential increase in child pornography material on Facebook, for example – even though Facebook itself stated that 90 percent of all reports come from material previously distributed[251].

The European Commission, led by Ylva Johansson, received criticism from all directions. Police chiefs pointed out that most of the material they receive today involves teenagers sending pictures to each other[252] and that such reports risk leading the police in the wrong direction. Scanning tests carried out by European police on existing material showed that 80-90 percent of all hits were false positives[253]. Now, moreover, 'new material' would be scanned – which would obviously mean an impossible administrative burden merely to distinguish between illegal images and holiday pictures from family days on the beach. The error rate would clearly be approaching 100 percent. For a European justice system that even today is unable to follow up all the tips[254] it receives, this would be devastating. And criminals would, of course, turn to illegal messaging services. No children would be helped. At the same time, every EU citizen would have spyware installed on their phones.

How did Ylva Johansson deal with this information? Not at all. Instead, like a scratched record, she continued urging everyone to "think of the children." She also ordered a survey that said 80 percent of the EU population supports Chat Control. The problem? The European Commission used its Eurobarometer series of public opinion surveys in a way that opened it to accusations of blurring the line between research and propaganda. When asked to comment on the Chat Control survey, the Max Planck Institute for the Study of Societies concluded that it had a political agenda and consisted of questions that were biased[255] to support the Commission's plans.

Ylva Johansson was employing blatant deception. She used incorrect figures and biased surveys. In interviews, she was populist and evasive. But she was forced to resort to these methods. Because it was never about the children.

American tech companies and security services behind the draft bill.

In September 2023, a major investigative article was published by three journalists: Giacomo Zandonini, Apostolis Fotiadis, and Luděk Stavinoha. After seven months of trying to get the European Commission to release public documents, they finally obtained a piece of material that allowed them to start putting together the puzzle. The puzzle that revealed the true stakes behind Chat Control[256]. The article, which was published in several European newspapers, included a letter in which Ylva Johansson wrote to Julie Cordua, CEO of the American company Thorn: "We have shared many moments on the journey to this proposal. Now I am looking to you to help make sure that this launch is a successful one."

Thorn is an American company, formed by actor Ashton Kutcher, which develops tools that scan for child pornography material. Thorn had sold software worth millions of dollars to the U.S. Department of Homeland Security. Ashton Kutcher himself had held video conferences with European Commission President Ursula von der Leyen, and had given lectures in the EU on how new technologies can scan encrypted content without looking at it. The picture of Ylva Johansson's digital sniffer dog suddenly became clear.

For several years Kutcher lobbied the European Commission (until he was forced to resign as chairman of Thorn's board after defending his acting colleague Danny Masterson when he was convicted of rape). He held meetings with others at the European Commission and had an extra close relationship with the Commission's Eva Kaili (until she was arrested for bribery and forced to leave her party[257]).

So here was an American company in direct contact with the European Commission. An American company that just happened to sell the technology that could be used if Chat Control was introduced. In addition, it was all based on a false premise. The technology Kutcher and Johansson talked about did not exist. Expert after expert condemned their talk of sniffer dogs[258].

And here's yet another seedy aspect to this scandal: in the EU transparency register, Thorn was registered as a charitable organization – despite selling the technology they were lecturing about in the EU. The trick of disguising organizations and corporations as charities would turn out to be a recurring motif.

Since the draft Chat Control bill was presented, Ylva Johansson has constantly referred to children's rights organizations that support her proposal. She has worked with them in a PR context, as a way to show how Chat Control has the support of independent, nonprofit organizations that care about children. A central organization in this work has been the WeProtect Global Alliance. When Zandonini, Fotiadis, and Stavinoha published their article, it turned out that the European Commission had been involved in founding this organization, and that it included representatives from both tech companies and security services in different countries. Ylva Johansson's colleague in the European Commission, Labrador Jimenez, was on the Board of Directors of WeProtect, together with Thorn's CEO Julie Cordua, representatives of Interpol, and government officials from the US and the UK (the latter simultaneously pursuing its own monitoring legislation, also using children as the battering ram). Thorn had put a great deal of money into WeProtect. The European Commission had contributed one million euros. In other words, it wasn't children's rights organizations that were supporting Ylva Johansson. It was lobbying organizations set up by the European Commission to get the bill through.

Children's rights organizations were established with the idea to "divide and conquer" the members of the parliament by deploying in priority survivors from MEPs' countries of origin.

The Board of Directors of WeProtect also included representatives from the Oak Foundation, who, in addition to their involvement in WeProtect, had also been involved in setting up ECLAG (another charity that supported the Chat Control proposal). ECLAG was launched just a few weeks after Ylva Johansson's draft bill was presented, and Thorn was also represented on this organization's board. And there was still another organization: the Brave Movement, an organization formed a month before the proposed Chat Control bill was introduced. Brave was launched with $10 million from the Oak Foundation and a strategy paper discovered by the journalists stated that "once the EU Survivors taskforce is established and we are clear on the mobilized survivors, we will establish a list pairing responsible survivors with Members of the European Parliament – we will 'divide and conquer' the MEPs by deploying in priority survivors from MEPs' countries of origin."

The Oak Foundation also appeared in an article carried out by the Intercept[259]. In 2023, an American organization called the Heat Initiative was formed. On paper, they were a "new child safety group" and the first thing they did was campaign for Apple to "detect, report, and remove" child pornography material from iCloud. Apple responded that this would be something that criminals would be able to exploit and that it could also lead to a "potential for a slippery slope of unintended consequences. Scanning for one type of content, for instance, opens the door for bulk surveillance."

The Heat Initiative did not like this answer and fought back with anti-Apple propaganda on large advertising billboards in American cities under the theme of 'think of the children.' But who was behind the Heat Initiative, besides the Oak Foundation? Heat was led by a former vice president at Thorn. The Intercept article also referred to the fact that Thorn was working with Palantir[260], the big-data company that helped the NSA mass-monitor the whole world[261] and was involved in the Cambridge Analytica scandal where Facebook users' private messages and data[262] were used to influence the presidential election on behalf of Donald Trump in 2016.

At the same time, the real organizations working to counter sexual crimes against children were wondering why the European Commission was refusing to talk to them.

In other words, the European Commission was involved in funding and starting up charities with the aim of exploiting existing victims to emotionally influence EU parliamentarians. In close cooperation with the tech company providing the technology that would be used in the implementation of the monitoring. Together with representatives of non-European security services. As part of a larger apparatus, where the same tactics were used to influence developments in the United States.

At the same time, the real organizations working to counter sexual crimes against children were wondering why the European Commission was refusing to talk to them. In the same investigative report, Offlimits, Europe's oldest hotline for vulnerable children, tells how Ylva Johansson would rather go to Silicon Valley to meet companies interested in making huge profits than talk to them.

The same is true of the technical experts. Matthew Green, Professor of Cryptography at John Hopkins University, said: "In the first impact assessment of the EU Commission there was almost no outside scientific input and that's really amazing since Europe has a terrific scientific infrastructure, with the top researchers in cryptography and computer security all over the world."

However, Europol was involved in drafting the law, together with security services from other countries[263]. In July 2022, Europol wrote that it wanted to be able to use scanning and surveillance for purposes other than sexual offenses against children. The European Commission responded that it understood the wish but that it had "to be realistic in terms of what could be expected, given the many sensitivities around the proposal." Thorn was also clear in understanding that the scanning could later be used for other purposes[264]: "When considering regulation or legislation on encryption it should not be done solely focusing on CSAM. Solutions for detection in encrypted environments are much broader than one single crime," the company wrote in one document[265].

It was later revealed that Europol was looking for unfiltered access to the scanned material[266]: "All data is useful and should be passed on to law enforcement. There should be no filtering by the [EU] Centre because even an innocent image might contain information that could at some point be useful to law enforcement."

When articles were published about the EU Commission's horrifyingly undemocratic approach, Ylva Johansson's office at the European Commission responded with illegal micro-targeting and propaganda on social media.

European Parliament: "the commission wanted mass surveillance."

So here was the European Commission, working on legislative proposals together with a Europol that wanted access to all surveillance, regardless of whether it contained something illegal or not – simply because it could be useful to have. In other words, it really wasn't about the children.

When articles were published about the EU Commission's horrifyingly undemocratic approach, Ylva Johansson's office at the European Commission responded by advertising on the platform X (formerly Twitter). They targeted advertisements (pro Chat Control) so that decision-makers in different countries would see them, but also so that they would not be seen by people suspected to be strongly against the proposal. The advertising was also targeted on the basis of religious and political affiliation and thus violated the EU's own laws regarding micro-targeting[267].

Ylva Johansson was being summoned to a hearing in the European Parliament, where an almost united European Parliament was massively critical of her approach.

Officials at the highest EU level thus used data collected by big tech to try to create illegal filter bubbles designed to push through a mass surveillance proposal. The whole thing ended with Ylva Johansson being summoned to a hearing in the European Parliament. An almost united European Parliament was massively critical of Ylva Johansson and her approach. She was grilled about Thorn's interference and about the targeted ads and the EU Ombudsman denounced the European Commission's unwillingness to share public documents

regarding the relationship with Thorn (the European Commission had assumed these would be classified because they risked undermining commercial interests …) Ylva Johansson's answer? "Think of the children."

In November 2023, the European Parliament's statement was delivered[268]. In an almost historic consensus, all the groups in the Parliament stood together and said "No" to the bill. At the press conference, representatives from the Parliament said[269]: "This is a slap in the face of the Commission, what we've tabled. The Commission wasn't focusing on protecting children but wanted mass surveillance." Patrick Breyer, who has been the most active opponent in the EU Parliament, called it a victory for the children, adding "They deserve an effective response and a rights-respecting response that will hold up in court."

Breyer was referring to the fact that Chat Control would most likely not hold up in court if the bill had been passed. Just a few months later, a ruling from the European Court of Justice[270] ruled that authorities do not have the right to demand access to end-to-end encrypted communications.

The Parliament's clear stance against chat control did not mean the fight was over. In the EU, two bodies are involved in the adoption of legislative proposals made by the EU Commission: the European Parliament and the Council of Ministers. Unfortunately, in the Council of Ministers, the tone was different. While the Parliament strongly opposed the proposal, unified in its stance, the Council continued to struggle to reach a common position. Time and again, they tried to come up with compromise proposals that would essentially result in the implementation of chat control. However, it became evident that not even the Council of Ministers believed in Ylva Johansson's digital sniffer dog, as parts of the Council proposed[271] that scanning should be excluded for politicians, police and intelligence services, as

well as anything classified as ”professional secrets.” Obviously, there were politicians who were afraid that their secrets would leak, but who had no issue with mass surveillance of the broader population. Patrick Breyer was clear in his response: “these people are aware that Chat Control involves unreliable and dangerous snooping algorithms – and yet they are ready to unleash them on us citizens.”

As a unified stance from the Council of Ministers was delayed, the deadline Ylva Johansson had mentioned in the debates was approaching. She had repeatedly argued that the EU would ”go dark” in the fight against criminals if chat control was not adopted – since the current legislation (the voluntary scanning) would expire in the summer of 2024. Did she then go public in the summer of 2024 and declare it was over? Of course not. She quickly and easily did what had previously been completely out of reach in her argumentation: she extended the previous legislation.

New attempt at mass surveillance via the Going Dark initiative.

While the EU member states in the Council were trying to come up with various compromise proposals to implement chat control, they were also working on a plan B and new attempts for mass surveillance legislation. During Sweden’s EU Presidency in spring 2023, a project called Going Dark was initiated. The idea from the Swedish Presidency was initially that a so-called High Level Expert Group would be launched. The task of putting together the group went to the European Commission, which immediately removed the ‘Expert’ label. Instead of a High Level Expert Group, a High Level Group was formed. As the Netzpolitik newspaper[272] put it: “Removing the word ‘expert’ is no small detail: special rules apply to Expert groups, for example when it comes to transparency. Rules that do not apply to High Level Groups.”

At the Going Dark meeting, a former FBI employee was present. He expressed his gratitude for the fact that the issue was being pursued within the EU and that solutions for legal access should be prioritized.

Once again, the European Commission chose to start the preparatory work linked to mass surveillance without allowing experts to play a serious part in the process. When the group met for the first time, it stated that the group's purpose was to discuss methods[273] to achieve "access to data for effective law enforcement, based on and guided by the inputs from the EU Member States."

Some challenges were identified as particularly pressing: access to encrypted material (both stored data and communication), data storage, location data, and anonymization (including VPNs and Darknets).

The group was divided into three working groups: the first would work with access to data on users' devices (computer and mobile), the second group would focus on access to data in the services' systems (messaging apps, for example), and the third group would discuss access to data in transit.

According to the minutes of the meeting of the Swedish Parliament's Committee on European Union Affairs, the group worked "to present effective recommendations for the accession of the new Commission in 2024 and for those recommendations to be implemented."[274]

Future legislative proposals from the European Commission could thus be assumed to be about providing access to data on users'

devices and in the messaging services' systems, and to data in transit. Patrick Breyer, who had worked hard to counter Chat Control, said the group was just an extension of past offensives and that Going Dark was working to introduce illegal mass surveillance[275]. When he requested documents from the group's meetings and a list of the attendees, he received a document with the information blacked out as if classified. The European Commission had thus put together a working group aiming to achieve mass surveillance of the broader population while not being transparent about who was part of the group. It was like a scratched record. Gone was the old excuse "think of the children", but the goal was the same.

However, some transparency was obtained through the Swedish Ministry of Justice, which at Mullvad VPN's request provided both meeting notes and information about the Swedish representatives present at the meetings.

The first Going Dark meeting was led by two people. One was Olivier Onidi, who is Deputy Director General directly under Ylva Johansson in the European Commission. Onidi has expressed that the "valuable" thing about Chat Control is "to cover all forms of communication, including private communication"[276], and he defended Ylva Johansson and Chat Control when he said: "I think it's totally unfair to point this out as a mandatory inspection of all private communications. That's not what you have in front of you. This proposal is a huge improvement over the current situation."[277]

Onidi has also been questioned for his meetings with the American company Palantir[278] (notorious for its involvement in US authorities' illegal mass surveillance).

The second person who led the first Going Dark meeting was Anna-Carin Svensson, international chief negotiator at the Swedish Justice Department, who, according to WikiLeaks documents in 2010, allegedly urged the US State Department and the FBI to con-

tinue with the current informal exchange of information between the countries instead of signing formal agreements. According to the American representatives at the meeting, it was about withholding information from the Swedish Parliament[279]:

"She believed that, given the Swedish Constitution's requirement to present matters of importance to the nation to the Swedish Parliament, and in light of the ongoing controversy over the newly decided FRA law [FRA, Försvarets radioanstalt, the Swedish National Defence Radio Establishment, is a Swedish government signals agency], it will be politically impossible for the Minister of Justice not to let the Parliament review any data exchange agreements with the United States. In her opinion, the publication of this could also jeopardize the informal exchange of information," the leaked documents said.

According to the documents, Anna-Carin Svensson asked the FBI if they could not continue to make use of the strong but informal arrangements. When the documents leaked, Svensson denied everything and stated: "I cannot be held responsible for how Americans express themselves."

From the Swedish side, the Ministry of Justice was represented at the Going Dark meetings, but so was the Swedish Security Service (Säpo) and the Swedish Police Authority. Together with representatives from the other Member States, they used the High Level Group meetings to discuss how, through legislation, encrypted services could be required to provide data in readable format. Several Member States argued that "the working groups needed to look at solutions that involved 'legal access through design'." This was something that pleased American representatives.

At the Going Dark meeting on November 21, 2023, a former FBI employee was also present, who said that "solutions for legal access should be prioritized" and that "companies needed to have a responsibility and follow the same rules." As a former FBI employee, he also

expressed "his gratitude for the fact that the issue was being pursued within the EU."

European police chiefs: we cannot accept criminals using secure communications.

The Going Dark meetings resulted in an outcry from the assembled police chiefs of Europe. In April 2024 Europol published the challenge[280] "European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out." The declaration was a "direct extension of the Going Dark initiative"[281] and, together, the European police authorities were clear that although encryption is "a means of strengthening the cyber security and privacy of citizens ... we do not accept that there need be a binary choice between cyber security or privacy on the one hand and public safety on the other. Absolutism on either side is not helpful."

It was as if Ylva Johansson's sniffer dog had caught the scent again. In the absence of expertise, the Going Dark initiative tried to magic away the fact that end-to-end encryption is absolute – either you have secure communication or you don't.

Although the UN classifies encryption as a human right, the Going Dark initiative and the European police force were fighting to smash end-to-end encryption.

The assembled police chiefs claimed there were two key factors for achieving online security[282] – which turned out to be direct repetitions of the reasoning in the Going Dark discussions. Number 1: so-called legal access to the tech companies' stored data. Number 2: real-time scanning of illegal activity in tech companies' services.

Naturally, they said, all this would be done under strong protection and supervision.

Stefan Hector, a representative of the Swedish Police Authority, said that "a society cannot accept that criminals today have a space to communicate safely in order to commit serious crimes." A week later, it was revealed that the Swedish police had been infiltrated and were leaking information to criminals.[283]

Although the UN classifies encryption as a human right, the Going Dark initiative and the European police force were fighting to smash end-to-end encryption. Their first move actually came as a reaction to Meta rolling out exactly such encryption.

Europol's move was only an initial indication. At the end of May 2024, the Going Dark initiative resulted in 42 recommendations[290] to the European Commission. The document notes that encryption adds a level of complexity when it comes to accessing real time content data, specially from messaging services implementing an end-to-end Encryption. It states that law enforcement need access to data en clair (i.e. in plain text) through "lawful access without weakening privacy." The Going Dark initiative emphasizes the principle of "security through encryption and security despite encryption" as a central tenet.

The Going Dark initiative shows the same tendencies as the chat control proposal. Once again, experts have been excluded from the discussions, and ministers and police representatives have once again missed the main point: either end-to-end encrypted communication is private and secure, or it is not.

The solution sought by the Going Dark initiative (just like chat control) is scanning that occurs before the communication is sent. They argue that this method does not break the end-to-end-encryption. Who cares? It breaks the entire purpose of end-to-end-encryption. If communication is scanned before it is sent, it is not private and secure.

The Going Dark initiative's 42 recommendations discuss stricter consequences for messaging services that do not provide "lawful access" to their data. With the principle of "security through encryption and security despite encryption", two methods for such access are obvious. The Going Dark initiative are either looking for so-called backdoors to the systems – where authorities have access to the services' systems to look at the data, or an extra key to the end-to-end-encrypted communication. Or they are looking for so-called client-side scanning, a scan that occurs in the user's app on the computer or phone itself. Client-side scanning could also occur on the operating system itself – which would be very pleasant for authorities since everything happening on the phone could be monitored in one sweep. Similar to how Microsoft has begun developing its feature Recall[291], a feature developed to take a screenshot of the screen every few seconds.

Implementing this type of state spyware on EU citizens' phones would not only mean that everyone's privacy is lost. It would also lead to significant security risks. By now, mass surveillance advocates should know this. The echoes from the chat control debate are literal. But it is also an echo of an older battle.

The Going Dark initiative seeks legislation that has been deemed illegal and violates human rights. It is a late ripple effect following Snowden's revelations, which changed the internet in many respects.

The Going Dark initiative is really just an extension of the so-called crypto war (the war against encryption) that US authorities have

been involved in since the internet began. As Signal's CEO Meredith Whittaker said in a keynote speech[284]:

"Encryption was essential for the commercial internet. But law enforcement and security services saw any network resistant to government surveillance as a threat and a problem."

The US authorities have already tested the backdoors that the European Going Dark initiative is now seeking. They have seen the evidence: it is impossible to implement backdoors in a secure way, without hostile states or hackers being able to exploit them. Edward Snowden revealed that the NSA spent $250 million a year[285] getting tech companies to install backdoors in their services, which also exposed the risks of backdoors. In 2010, Chinese hackers managed to use a Google backdoor[286] to get into Gmail. The same thing happened in 2005, when state surveillance of Vodafone was exploited[287] by outside actors to bug the Greek Prime Minister, his Foreign Minister, Justice Minister, and a hundred other government officials.

The Going Dark initiative might go for so-called client-side scanning instead; scanning directly in the apps on users' phones and computers, or even scanning the entire operating system. Besides the fact that this surveillance method would bring state spyware to everyone's phones, it is also doomed to fail from a security perspective. It would not be possible to keep the data private and secure. We know this because Apple, one of the world's most technologically advanced and wealthy companies, has poured incredible resources into figuring out if it can be done in a secure and private way. But when Apple made its effort public, it took hackers just two weeks to break in. Apple abandoned the attempt and continue to say no to anyone who asks them to try this again – simply because it's too easy to hack systems where client-side scanning is involved[288].

The Going Dark initiative's ambition to introduce backdoors and client-side scanning are not compatible with EU laws and human

rights. But instead of working on proposals that do not violate human rights, the Going Dark initiative will focus on propaganda to push through its upcoming legislative proposals. Leaked documents[292] emphasize the importance of 'setting the right narrative' and developing a 'communication strategy that underlines that the recommendations aim to protect fundamental rights.

A quick recommendation from Mullvad VPN: develop proposals that do not violate human rights – then just show them to the world.

The Going Dark initiative seeks legislation that has been deemed illegal and violates human rights. It is a late ripple effect following Snowden's revelations, which changed the internet in many respects. After Snowden's whistleblowing, encrypted websites (https) became standard. End-to-end encrypted messaging services like Signal saw a widespread increase in popularity. Apple started using strong encryption in its operating systems. From having virtually free access to people's internet traffic (if they didn't use a trustworthy VPN, that is) and from having been able to read people's messages in plain text, the internet now became more difficult for US authorities to mass monitor.

In her speech, Meredith Whittaker points to an important point: "Strong encryption was an important win. But the result of this win was not privacy. Indeed, the legacy of the crypto wars was to trade privacy for encryption – and to usher in an age of mass corporate surveillance. Because the power to enable – or violate – privacy was left in the hands of companies, not those who relied on their services. Companies that were incentivized to implement surveillance in service of advertising and commerce."

For more than twenty years, so-called commercial mass surveillance has created some of the richest companies in the world. The fact that Meta is rolling out end-to-end encryption doesn't mean they have abandoned their business model. But it was still sufficient for

the European police chiefs, cheered on by the US authorities, to make a joint declaration demanding legal access to the content in secure and private communications. Meredith Whittaker again:

"In my view, the ferocity of the current attack on end-to-end encryption, and other privacy-preserving technologies, is very much related to a desire by some in government to return to the less fettered access to surveillance that they see as having lost post-Snowden."

We can see the attack coming in Europe right now. But the movement is based in the United States. Back in 2014, just a year after Snowden's revelations, FBI Director James Comey spoke[289] of how "the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place."

The US authorities, which in 2014 had recently been caught spying on the entire world, used a particular expression when they began lobbying to regain access to easily controlling everything and everyone. FBI Director Comey talked about "Going Dark."

“The ferocity of the current attack on end-to-end encryption, and other privacy-preserving technologies, is very much related to a desire by some in government to return to the less fettered access to surveillance that they see as having lost post-Snowden.”

Meredith Whittaker, CEO Signal.

THE CONSEQUENCES OF MASS SURVEILLANCE: HOW THE COLLECTED DATA IS USED

Monitoring your internet behavior has consequences – you may just not be seeing them yet.

Commercial and state mass surveillance collects absurd quantities of data about people all over the world. But what is all the data used for? When your internet behavior has been mapped, what might it lead to?

Quite often, we encounter people who say something like: "Yeah, yeah, so they're collecting loads of data, but why should I worry?" There are several answers to that question, but one of them is quite simply that data can leak. The 'normal internet user' may not care that personal data is stored by one of the world's biggest companies or by a state authority, but they may have more of a problem with personal information ending up in what's usually called 'the wrong hands'. You may not be worried about a pharmacy storing the medicines you buy, but think it feels creepy when the headlines scream about data breaches.[151] Because it's exactly that simple: Collected data equals data that can leak. If the state, a company or an organization

hold sensitive data, they are responsible for keeping it secure in an unpredictable future. That's a difficult task, particularly when technology is developing quickly and companies and authorities (normal authorities, not the ones carrying out mass surveillance) are struggling to keep up. Over and over again, history has shown how databases are used in the worst possible way when new leaders come to power. We have far too often seen hackers and enemy powers gaining access to data they absolutely shouldn't have. And how carelessness, poor structures and human factors have led to leaks. Our attitude to this is extremely simple, and our message to anyone storing data is clear: minimize your data storage. Data you don't have can't leak.

But unfortunately right now the recurring scandal headlines about data leaks aren't the big problem. The big problem is that there's essentially a constant leak, when commercial and state mass surveillance deliberately collects data. But what happens next? Apart from the fact that you get annoying ads targeting you, how is your data actually used?

The short answer when it comes to state mass surveillance is that several countries in the world have the capacity to look at your collected internet behavior, whenever they like. Depending on where you live, this can have disastrous consequences for you.

You may think: who cares what websites I click on? But if you live in the USA, insurance companies care. They use purchase histories to bump up the prices for your premiums.

When it comes to the commercial mass surveillance companies, there's also a very short, simple answer to what they do with your

data: they sell it. In 2021, it was revealed that data brokers had purchased location data from Life360[152], an app in which 33 million parents keep track of where their children are by tracking the child's phone. The following year, a lawsuit was brought against Kochava, another data broker, for having tracked hundreds of millions of people and sold sensitive data about their location.[153]

Depending on the country you live in, your internet provider may also log your traffic and share it through a variety of business agreements. A report from the American Federal Trade Commission (FDT)[154] described how at least six large American internet providers were sharing their customers' location data with third-party companies. The report noted that even though several of the ISPs promised not to sell consumers personal data, they allowed it to be used, transferred, and monetized by others and hid disclosures about such practices in the fine print of their privacy policies.

And this is a tactic even the biggest tech companies employ. Meta and Google may not sell their (your) data, but they exchange it freely.[155] But above all, the tech giants use data collection to optimize their advertising tools. Meta and Google have become two of the highest valued companies in world history through revenues from their advertising networks, and their business concept is clear – it's all about mapping your behavior and predicting what you're going to want in the future to tailor ads as accurately as possible.

Data on medical histories and sexual orientations is sold and exploited.

You may be asking the question 'Who cares if Facebook keeps track of what sites I click on?' You may also like seeing ads tailored to you. But it may not feel quite as innocent when the data is bought by an insurance company, for example.

The FDT has reported how data is sold to insurance companies, which in turn use purchase histories to raise the premiums for couples paying for couples therapy.[156]

Another example is health apps sharing data with hundreds of different partners about users' herpes, HIV and diabetes[157], and data brokers that can easily construct profiles under categories such as 'depressed'. The question is what happens to people who are cataloged like this: do their insurance premiums go up, do they become the target of information and ads that can lead to them becoming addicted to medication, does the interest rate on their mortgage go up?

Another example: the Catholic priest exposed as homosexual through location data sold by a data broker.[158]

It's incredibly easy to buy data from data brokers, data that can be de-anonymized. The consequences of this include vulnerable women having their real-time location data revealed to stalkers.[159] And as early as 2013, it was possible to purchase information about people who had been raped and lists of people with drug and alcohol dependencies.[160] Once again: who are the buyers and how is the information being used? It's difficult to speculate any positive outcomes from this type of data list.

It's a fact in today's world that socially vulnerable people suffer as a result of the collection and sale of data. But if you want to contemplate the ultimate outcome of this development, you can look at China and the country's social credit score system.

China's social credit score system gives you minus points if you play too many computer games.

There are many misconceptions about the Chinese social credit score system. The most common one can be seen in the last sentence: because there isn't only one Chinese social credit score system. As a

“There is no single, nationally coordinated system. There are several. But if [the Chinese system] does come together as envisioned, it would still be something very unique. It’s both unique and part of a global trend.”

Mareike Ohlberg

researcher Mareike Ohlberg from the Mercator Institute for China Studies expressed it in an article in Wired.[161]

She says that the idea itself isn't a Chinese phenomenon, and neither is the use and misuse of collected data and behavioral analyses. Nor is there a single, nationally coordinated system, but instead several different pilot projects that don't work in exactly the same way. But if they manage to put them together, as they intend, it will create something truly unique. In this way, says Ohlberg, the Chinese social credit score programs are unique but also part of a global trend.

In other words, the Chinese social credit score programs record slightly different things, but overall cover everything from late payment of your bills and running a red light to playing your music too loud on a train or making a scene in a taxi. You probably recognize this type of scoring system from the western world's credit checks and the ratings in services such as Uber. What makes China stand out is perhaps the ambition to collect everything into one system. For example, Mareike Ohlberg describes the Chinese city of Rongcheng, which gave every inhabitant 1000 points to start with, and where deductions take place, for example when residents commit a traffic violation, but where they can earn more points by giving money to charity.

Several of the pilot projects are being run by giants such as Alibaba. Sesame Credit runs one of them, and has become famous for collecting data about its 400 million customers and allocating scores based on how much time they spend on video games and whether or not they are parents.[162] The social credit score is included as a parameter in the company's dating app.

Another well-known example is how investigative journalist Liu Hu was refused the right to buy an airline ticket because he had been allocated the status 'not qualified'.[163]

Parallels with the fictional series Black Mirror[164] are only too evident. Of course, you can joke about the irony in your social score

falling because you went to the wrong parties or lost your temper in the grocery store. The problem is that this is happening in reality, here and now, and that the ultimate goal of this type of mass surveillance is total control over people. And of course it will be worst for those who are already the most vulnerable in society. But you don't need to look as far as China to discover truly frightening contemporary examples.

Perhaps you'll say that you 'have nothing to hide'. But what happens when the laws change?

When people justify mass surveillance with 'I have nothing to hide', there are several arguments that disprove their reasoning. But nothing has put as many holes in this argument as contemporary events in the USA. A big problem with 'I have nothing to hide' is that it isn't unchanging. You may change your political view, become an activist and suddenly find yourself, through your online searches, getting extra attention from the authorities. You may become depressed, buy tons of junk food and see your insurance premiums rocket. Perhaps you're homosexual and find a partner in a country where it's prohibited by law.

Perhaps you live under the delusion that you 'have nothing to hide' but then the law changes and you're a criminal. In 2022, life suddenly changed for millions of American women when they could no longer google for abortion doctors, buy abortion pills online or visit abortion clinics (with their phone in their pocket) without risking it becoming proof in a potential indictment against them. Suddenly they did have something to hide, and the USA's digital infrastructure means the odds are stacked against them. If, as a society, you've long permitted the internet to become a place where both state and commercial actors can map human lives, it becomes tough for those humans when the law suddenly takes a new turn.

Immediately after Roe vs Wade was overturned in June 2022, we saw one story after another about women deleting their pregnancy

apps (at least the women who used them as aids to avoid becoming pregnant). And that was a sensible decision by all of them, given how researchers have reported that the majority of pregnancy apps share large quantities of personal data with other companies.[165]

The tone in the discussions about location data also changed. In 2019, the New York Times released its Privacy Project.[166] The newspaper had obtained a dataset containing location data for more than 12 million Americans. The data contained more than 50 million location pings that were claimed to be anonymous. And yet it took only a few minutes for the newspaper to work out which of the movement patterns belonged to Donald Trump.[167] Of course, when it comes to location data it's child's play to de-anonymize it, because there aren't many people who sleep in the same place as you and then go to the same workplace as you.

Now take that type of database and pull out all the location pings linked to an abortion clinic and then follow their journeys home. This isn't a hypothetical exercise. Vice reported that for a measly 160 USD it's possible to buy a full week's list of the people who visited a specific clinic linked to pregnancy[168] – and that it's even possible to see where the visitors came from and where they went afterwards. This is data that absolutely anyone can buy.

We've already seen the perfect storm caused by a combination of data brokers and their dubious records, the willingness of US states to imprison women who have abortions and greedy bounty hunters. In Texas and Oklahoma, an inhabitant – absolutely any inhabitant whatsoever – can get up to ten thousand dollars' reward by reporting women who have broken the abortion laws.[169]

A digital infrastructure has been constructed that makes it possible to map peoples' lives and work out what they will do next. And in a country like the USA, the authorities have access not only to their own tools, but also to the commercial companies that follow every

“The harsh reality is that while we’re now worried about women who seek abortions being targeted, the same apparatus could be used to target any group [...] at any moment, for any reason that it chooses.”

Shoshana Zuboff

step we take. Once such a system is in place, it's very easy to shine the spotlight wherever you want. As an article in the New York Times puts it[171]: "A woman who regularly eats sushi and suddenly stops, or stops taking Pepto-Bismol, or starts taking vitamin B6 may be easily identified as someone following guidelines for pregnancy. If that woman doesn't give birth she might find herself being questioned by the police, who may think she had an abortion."

AI systems have even been developed to calculate the probability that young girls will become pregnant.[172] In a 2018 collaboration between Microsoft and an Argentinian organization, algorithms were developed that they claimed were 86% accurate at calculating which girls would become pregnant within a six year period. Behind the Argentinian organization was a well-known anti-abortionist.

The abortion issue is a clear example of how 'I have nothing to hide' can change. But that's 'only' one example of a much more widespread phenomenon. As Shoshana Zuboff said in an interview in the Washington Post[173]:

"The harsh reality is that while we're now worried about women who seek abortions being targeted, the same apparatus could be used to target any group or any subset of our population – or our entire population – at any moment, for any reason that it chooses. No one is safe from this."

The digital infrastructure of today can map the lives of people worldwide. But it could get worse. With the development of AI, we risk ending up in a society where everyone's online behavior is analyzed at a much faster pace. There is much to be said about AI, but if artificial intelligence is good at anything, it's sorting through large amounts of data. As Edward Snowden put it during a talk in 2024:

"Metadata could be collected automatically by ingesting the world's internet communication through these machines but somebody still had to put their cup in the big bucket, pull it out and lay

it on their desk and make sense of it. Machine learning models are going to change this. In my opinion, this is already being done. We simply don't have the evidence yet, it's going to be testing, it's going to be development, we don't know how it's being applied, when it's going to be truly operational – but it's fantasy to imagine that they're not doing this, and there is zero regulation that I'm aware of in the United States to prevent this. Nobody is thinking about what these agencies are doing, and we're not just talking about the NSA here, we're not just talking about the FBI, we're talking about the IRS right, and it's not just the United States, it's every country. You may go 'oh I love the United States government doing this, I hope they spy on me as much as possible', well what about China, what about Russia, what about North Korea, what about Iran, what about every little government that you don't like, that you don't agree with. Suddenly they can have every life of every person every day at every moment on a live feed being interpreted at machine speed. And then you start feeding those inferences into a decision-making process. This is the reason that I bring up the protesters at Columbia University, the protesters in Canada, it doesn't matter whether you're a liberal, it doesn't matter whether you're a conservative, if you stick out, if you stand out, you are going to become non-normative, or rather, anomalous."

THE CONSEQUENCES OF MASS SURVEILLANCE: HOW DATA COLLECTION THREATENS A FREE SOCIETY

Both state and commercial mass surveillance risk transforming free democracies into surveillance states.

Authoritarian states use mass surveillance to control the population. Even in democratic countries, we see direct consequences of collecting absurd amounts of data. But there are also less visible effects: both state and commercial mass surveillance show signs of being able to transform free societies into the complete opposite.

Mass surveillance equals control. We find the most obvious examples of this in countries such as Iran where the internet is censored, the inhabitants' online behavior is controlled[174] and where so-called smart cameras identify women who aren't wearing a hijab.[175]

Or in Russia where the authorities combine mass online surveillance[176] with a vast number of surveillance cameras using facial recognition to catch journalists and people critical to the regime.[177]

Even worse is China with its total surveillance of people's online lives[178], the censorship tool known as the Great Firewall of China[179] and persecution of people taking part in protests.[180] And not least the

country's surveillance cameras, using technology claimed to be able to determine a person's ethnicity.[181] In 2018, Huawei and the China Academy of Sciences applied for a patent for exactly this type of AI camera.

China's uses of this type of surveillance technology include persecuting the Uyghur people in Xinjiang province. They are registered using technology dubbed 'racial AI', and Human Rights Watch has reported[182] that during a nine-month period the state carried out 11 million searches on the phones of almost half of the 3.5 million inhabitants of Urumqi, Xinjiang's capital city. The result of this mass surveillance? Documents obtained by CNN in 2020 showed that millions of Uyghur were first monitored and then imprisoned[183] in work camps on totally fabricated grounds. At the same time, it's been reported that China tested another type of new technology on the Uyghur, where AI cameras using 'emotion detection' were used to reveal emotional states.[184] Naturally, the Chinese state denies this and in an interview responded to the BBC that in China, "People live in harmony regardless of their ethnic backgrounds and enjoy a stable and peaceful life with no restriction to personal freedom".

Investigative journalist Liu Hu, who was denied the ability to travel on public transport because he had scored poorly in one of China's social credit score systems, has another perspective. As he told the BBC[185]: "There have been occasions when I have met some friends and soon after someone from the government contacts me. They warned me, 'Don't see that person, don't do this and that'. With artificial intelligence we have nowhere to hide."

Perhaps you're wondering how China justified this new surveillance system that's now persecuting entire ethnic groups? Well, it was introduced after five people were killed in 2016 in what the state described as a terrorist attack.

“In 2019, 70+ countries were subject to social media manipulation campaigns. The number of global democracies has been declining since social media emerged around 2010.”

Center for Humane Technology

These countries have hit rock bottom. Things can always get worse for their populations, but we aren't talking about free societies here. The question is how far the world's democracies will follow in their footsteps.

There are hundreds of terrifying examples, even in countries classified as democratic. In both Europe and other parts of the world, we've seen how Pegasus spyware is used to target dissenters, political activists and journalist.[186] Mass surveillance in the USA is a chapter in itself, and Edward Snowden's revelations showed how extreme the country's authorities are when it comes to this activity.

This type of surveillance is reminiscent of George Orwell's dystopian 1984, with its telescreens, 'Big Brother is watching you'[187], thought police and a lack of freedom of speech. But there are other elements in the old dystopian books that accurately predicted other parts of our current situation. Like the propaganda and obvious fake news in 1984. Or like in Aldous Huxley's Brave New World[188] where people get by on happy pills (social media and dopamine rushes, anyone?), are clearly anti-intellectual (TikTok, anyone?) and believe they live a good life despite the fact that their freedom has in fact slipped through their hands.

Large parts of the world have already sunk into some kind of cross between these two dystopias. And the countries still classified as free democracies now have a choice: either a society based on control or a society based on culture.

We are already seeing how mass surveillance comes with disastrous consequences in countries classified as democracies. But mass surveillance isn't merely a symptom. It's also used to control development and steer free countries in the wrong direction. There is a risk that, hand-in-hand, state and commercial mass surveillance will water down democratic societies. This is something happening right here, right now. In 2019, 70+ countries were subject to social media

manipulation campaigns[189]. The number of global democracies has been declining[190] since social media emerged around 2010.

"We've created an entire global generation of people who are raised within a context where the very meaning of communication, the very meaning of culture, is manipulation."

Meta and Google have become two of the highest valued companies in world history thanks to income from their advertising networks and their business concept is clear. It's about mapping your behavior and predicting what you're going to want in the future to tailor ads as accurately as possible. And even better if they can steer your behavior in the desired direction. As Harvard professor Shoshana Zuboff writes in her book The Age of Surveillance Capitalism:

"Automated machine processes not only know our behavior but also shape our behavior at scale. In the thousands of transactions we make, we now pay for our own domination."

What Zuboff is talking about is, for example, Meta's AI system, which according to leaked documents[191], as early as 2018 had the capacity to collect thousands of billions of data points every day to produce 6 million behavioral predictions per second.

Tristan Harris, former design ethicist at Google and later founder of The Center of Humane Technology[192], expresses the same thing in the documentary Social Dilemma[193]:

"We're pointing these engines of AI back at ourselves to reverse-engineer what elicits responses from us. So, it really is this kind of prison experiment where we're just, you know, roping people into the matrix, and we're just harvesting all this money and data from all their activity to profit from. And we're not even aware that it's happening."

In the same documentary, Sean Parker, Facebook's first president, says the company was aware of what it was doing from the outset.

“We were all looking for the moment when technology would overwhelm human strengths. But there’s this much earlier moment. When technology exceeds and overwhelms human weaknesses. And this is checkmate on humanity.”

Tristan Harris

"I mean, it's exactly the kind of thing that a hacker like myself would come up with. Because you're exploiting a vulnerability in human psychology. And I think that we… you know, the inventors, creators, it's me, it's Mark (Zuckerberg), it's Kevin Systrom at Instagram, all of these people… We understood this consciously, and we did it anyway."

The creators of the tech giants (at least, those who've left the companies) speculate that data collection and the AI engines analyzing billions of internet users could be the end of humanity. As Tristan Harris says:

"We were all looking for the moment when technology would overwhelm human strengths and intelligence. But there's this much earlier moment… when technology exceeds and overwhelms human weaknesses. This point being crossed is at the root of addiction, polarization, radicalization, outrage-ification, vanity-ification, the entire thing. This is overpowering human nature. And this is checkmate on humanity."

Jaron Lanier is one of the creators of virtual reality, but now he advocates for unplugging from social media for good.[194]

In a conversation with Jordan Harbinger, he agrees that "social media can manipulate your behavior and it puts your free will under threat. It contributes to this mass production of misinformation."

In Social Dilemma[195], he says:

"We've created a world in which online connection has become primary, especially for younger generations. And yet, in that world, any time two people connect, the only way it's financed is through a sneaky third person who's paying to manipulate those two people. So, we've created an entire global generation of people who are raised within a context where the very meaning of communication, the very meaning of culture, is manipulation. We've put deceit and sneakiness at the absolute center of everything we do."

Or as Shoshana Zuboff puts it in the documentary The Big Data Robbery[196]:

"One of the things that Chris Wiley (the whistleblower who revealed the Cambridge Analytica scandal) said when he broke this story with the Guardian back in 2018 is that we knew so much about so many individuals that we could understand their inner demons and we could figure out how to target those demons. How to target their fear, how to target their anger, how to target their paranoia and with those targets we could trigger those emotions. And by triggering those emotions we could then manipulate them into clicking on a website, joining a group, tell them what kind of things to read, tell them what kind of people to hang out with, even tell them who to vote for".

Absurd amounts of collected data and AI systems targeting human fears helped Trump win the election. Today, mass surveillance is used to monitor women who want to an abortion.

Each of us who lives with social media and in today's digital world should think about the personal profiles that AI systems create. Are they used in a positive or negative way? If someone is classified as depressed, does that person then see targeted content suggesting that they go out and run in the woods or ads for one medication after another? If somebody buys unhealthy quantities of soda, does that mean they get suggestions for an alternative lifestyle or a discount for Coca-Cola? For somebody who's started reading about conspiracy theories, do they get ads for books issued by the university or recommendations for sites about fake moon landings and how the Earth is flat?

“Let’s not be naive. Our government will be tempted to annex these capabilities and use them over us and against us. When we decide to resist surveillance capitalism right now [...] we are also preserving freedom and democracy for another generation.”

Shoshana Zuboff

A document leaked to The Australian[197] revealed that Meta had offered advertisers the opportunity to target 6.4 million younger users (children) during moments of psychological vulnerability, such as when they felt 'worthless', 'insecure', 'stressed', 'defeated', 'anxious', and like a 'failure'.

The same tactics used to sell products and services are used to influence users in a particular political direction. Shoshana Zuboff again[198]:

"Every aspect of Cambridge Analytica's operations was simply mimicking a day in the life of a surveillance capitalist". But instead of manipulating people for commercial purposes, they did it for political gain. Instead of a purchase, a vote. "Democracy is on the ropes in the UK, US, many other countries", says Zuboff. "Not in small measure because of the operations of surveillance capitalism."

Tristan Harris, who was formerly a design ethicist at Google but now runs The Center of Humane Technology, uses numbers to clarify how today's data collection and the prevailing social media world affect politics[199]: 9% of all tweets in the 2016 US Presidential Election were generated by bots. Ahead of the 2020 U.S. election, Facebook's top pages for Christian and Black Americans were run by troll farms.

And the algorithms that social media is based on are created to promote chaos: each word of moral outrage added to a tweet increases the rate of retweets by 17%, which accelerates polarization. Each negative word about political opponents increases the odds of a social media post being shared by 67%.

MIT has its own figures[200] for how fake news spreads faster than real news. And additional research has demonstrated that Facebook's algorithms pushed some users into 'rabbit holes', which Meta knew about but didn't do anything to prevent.[201]

In other words, we have a digital infrastructure that collects absolutely everything we do and which promotes radical and untrue

content. It's quite obvious that if you have such a system in place it will be exploited. Like when the company Cambridge Analytica (of which Donald Trump's chief strategist Steve Bannon was formerly a board member) obtained access to 87 million Facebook users' personal data (including private messages) that the company then fed into its own AI system.[202] Out came personal profiles that Cambridge Analytica then used to tailor digital content aimed at people undecided about how they should vote in the presidential election between Donald Trump and Hillary Clinton. The sponsored posts built on the recipients' fears, were designed in a radical way to trigger the algorithms[203] and contained clear fake news.[204]

In an interview, whistleblower Christopher Wylie[205] talked about the consequences:

"You are whispering into the ear of each and every voter, and you may be whispering one thing to this voter and another thing to another voter. We risk fragmenting society in a way where we don't have any more shared experiences and we don't have any more shared understanding. If we don't have any more shared understanding, how can we be a functioning society?"

In the Netflix documentary The Great Hack[206], Cambridge Analytica's CEO says it wasn't the only company involved in the election in this way. To this can be added the fact that Russian troll factories were once again causing havoc prior to the American election[207] and the information that Cambridge Analytica is said to have been implicated in 200 elections around the world.[208] A picture emerges of how commercial data collection has consequences far beyond targeted ads for that sweater you looked at that one time.

In other words, we've seen evidence of how collected data, together with algorithms and AI systems that build on people's fears and uncertainties, were used to spread fake news so Donald Trump could win the presidential election. Once in power, Trump changed

the abortion laws and now mass surveillance is being used to monitor women, who are facing the sudden realization that the abortion they want is now illegal.

In the documentary The Big Data Robbery[209], Shoshana Zuboff urges citizens of democracies not to be so naive.

"Our self-determination, our privacy are destroyed for the sake of this market logic. That is unacceptable. And let's also not be naive. You get the wrong people in charge of our government at any moment, and they look over their shoulders at the rich control possibilities offered by these new systems. And there will come a time when, even in the west, even in our democratic societies, when our governments will be tempted to annex these capabilities and use them over us and against us. Let's not be naive about that. When we decide to resist surveillance capitalism, right now while it lives in the market dynamic, we are also preserving our democratic future and the kinds of checks and balances that we will need going forward in an information civilization if we are to preserve freedom and democracy for another generation."

"Privacy is the fountainhead of all other rights. Freedom of speech doesn't have a lot of meaning if you can't have a quiet space, a space within yourself."

What Shoshana Zuboff is talking about is resistance that must come now, before it's too late. This is an important point. Because the infrastructure built today will be used by future governments. Because we don't know who will be coming to power. And because this type of surveillance society tends to come creeping in, hidden from the masses. Function creep is total in this area. As we all know, the road to hell is paved with good intentions and it's difficult to detect the bigger picture when it's being laid out one small jigsaw piece at a time. Every

obscure small law that's introduced may not represent a catastrophe, but together they're taking us in the wrong direction. And the ultimate destination is crystal-clear: when a country has introduced total mass surveillance, people begin self-censoring. When they can't be sure whether or not they're being monitored, they hold their tongues. In a Ted Talk, Glenn Greenwald, one of the journalists who met Edward Snowden in that Hong Kong hotel room and helped him get the word out, explains exactly how self-censorship is a highly developed control method that's been used for several hundred years.[210]

"In the 18th-century philosopher Jeremy Bentham set out to resolve an important problem [...] for the first time, prisons had become so large and centralized that they were no longer able to monitor and therefore control each one of their inmates. He called his solution the panopticon [...] an enormous tower in the center of the institution where whoever controlled the institution could at any moment watch any of the inmates. They couldn't watch all of them at all times, but the inmates couldn't actually see into the panopticon, into the tower, and so they never knew if they were being watched or even when. This made Bentham very excited. The prisoners would have to assume that they were being watched at any given moment, which would be the ultimate enforcer for obedience and compliance. The 20th-century French philosopher Michel Foucault realized that the model could be used not just for prisons but for every institution that seeks to control human behavior: schools, hospitals, factories, workplaces. And what he said was that this mindset, this framework discovered by Bentham, was the key means of societal control for modern, Western societies, which no longer need the overt weapons of tyranny – punishing or imprisoning or killing dissidents, or legally compelling loyalty to a particular party – because mass surveillance creates a prison in the mind that is a much more subtle though much more effective means of fostering compliance with social norms or

with social orthodoxy, much more effective than brute force could ever be."

In the same TED talk, Greenwald also talked about the cooling effect that mass surveillance has on society:

"When we're in a state where we can be monitored, where we can be watched, our behavior changes dramatically. The range of behavioral options that we consider when we think we're being watched severely reduce. This is just a fact of human nature that has been recognized in social science and in literature and in religion and in virtually every field of discipline. There are dozens of psychological studies that prove it."

Shoshana Zuboff[211]:

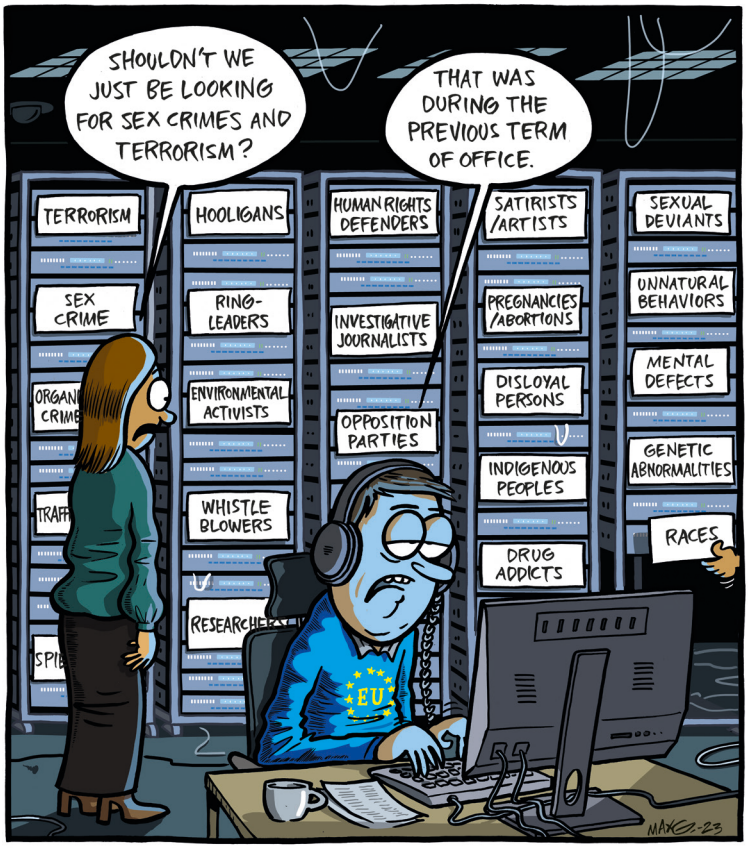
"Privacy rights enable us to decide what is shared and what is private. These systems are a direct assault on human agency and individual sovereignty as they challenge the most elemental right to autonomous action. Without agency there is no freedom, and without freedom there can be no democracy."

Edward Snowden[212]:

"Privacy is what gives you the ability to share with the world who you are on your own terms for them to understand what you're trying to be and to protect for yourself the parts of you that you're not sure about that you're still experimenting with. If we don't have privacy what we're losing is the ability to make mistakes we're losing the ability to be ourselves. Privacy is the fountainhead of all other rights. Freedom of speech doesn't have a lot of meaning if you can't have a quiet space, a space within yourself, within your home to decide what it is that you actually want to say."

It's actually quite simple. Either we have a society where people have the right to their own thoughts, their own private conversations and space to test out their ideas. A free society, where development and change are possible. Where power can be challenged,

examined and replaced. Or we have a closed society where you never know whether or not you're being watched. Either we continue step-by-step towards undemocratic societies. Or we instead try to uphold Article 12 of the universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy".



THE CONSEQUENCES OF MASS SURVEILLANCE: WE ALL HAVE SOMETHING TO HIDE

To those of you with nothing to hide:

One day you might have. Because you don't make the rules.

The most common argument used in defense of mass surveillance is 'If you have nothing to hide, you have nothing to fear'. Try saying that to women in the US states where abortion has suddenly become illegal. Say it to investigative journalists in authoritarian countries. Saying 'I have nothing to hide' means you stop caring about anyone fighting for their freedom. And one day, you might be one of them.

This chapter is aimed at those of you who say you have nothing to hide. We've written it because it's the most common argument from people indifferent about mass surveillance – or who even advocate it. The long version of the expression goes 'If you have nothing to hide, you have nothing to fear', and it's been reeled off by authorities for a hundred years. And slightly remixed versions have also been used by the commercial mass surveillance companies. By Mark Zuckerberg and by Google's former CEO Eric Smith[213], who said: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place".

To start with, this is a phrase that sounds very different depending on what country you're in. In many places in the world, there are large numbers of people who actually do have something to hide. Like investigative journalists persecuted in authoritarian countries. Like homosexuals in countries where it's forbidden. Like political opponents monitored by totalitarian states. Like women looking for an abortion in states that have made it illegal. Like people living under protected identities and who don't want to risk their true identity leaking out.

Saying "if you have nothing to hide you have nothing to fear" is unrealistic and equates to not caring about the individuals among us who do actually have something to fear – many of these people risk their lives if they can't conceal who they are, what they believe, and what they're fighting for.

"If you have nothing to hide" is a way of thinking that's incredibly shallow. In a world that thinks only criminals have anything to hide, there can be no business confidentiality. In such a world, sensitive health data risks leaking every day. Not to mention politicians in possession of information that mustn't come into foreign hands. Or perhaps those in power shouldn't be subject to the same rules as the rest of the population?

The argument "if you have nothing to hide, you have nothing to fear" is fundamentally backwards. Citizens shouldn't need to explain to the state (or to companies) why they don't want to be monitored. On the contrary, the state should have to explain why it's digging around in someone's private life.

Because in fact we all something to hide: our private life, which is nobody else's business, provided you aren't suspected of a crime and an order has been issued by an independent, free and democratic court stating that proportional surveillance is warranted.

From politicians and authorities, the expression often comes with a supplement: "To keep us all safe, we must relinquish a little of our

privacy". But as Benjamin Franklin once said[214]: "Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety". Or as American cryptographer and security expert Bruce Schneier describes it[215]:

"Too many wrongly characterize the debate as 'security versus privacy'. The real choice is liberty versus control. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide."

Bruce Schneier is onto something important: a state should have absolute power.[216] He also gives us two essential reminders and an equally important question: Privacy protects us from abuses by those in power. Absolute power corrupts absolutely. And who watches the watchers?

Edward Snowden argues for the same thing under the slogan: Privacy is for the powerless. Transparency is for the powerful.[217]

"You don't need to say why you want to be left alone by the state. It is the natural state of being that we are allowed in a free society to be free. If they want to restrict and monitor our activities it really changes the nature of human society."

When you say you have nothing to hide, you're making a bet that you never will have in a system that changes but never forgets.

The foundation of a democratic society is that its citizens have the right to personal privacy. But let's say that you still think mass surveillance is okay, because 'you have nothing to hide'. The problem with 'nothing to hide' is that it's not an unchanging status. Just ask the women living in US states who thought they had nothing to hide – until the law was changed overnight and it was no longer legal for them to have an abortion.

Glenn Greenwald was one of the journalists who helped Edward Snowden get the word out. In a Ted talk entitled Why Privacy Matters[218], he illustrated how mass surveillance takes no account either of changes in those in power or those being monitored.

"When you say, 'somebody who is doing bad things', you probably mean things like plotting a terrorist attack or engaging in violent criminality. A much narrower conception of what people who wield power mean when they say 'doing bad things'. There's an implicit bargain that people who accept this mindset have accepted, and that bargain is this: if you're willing to render yourself sufficiently harmless, sufficiently unthreatening to those who wield political power, then and only then can you be freed of the dangers of surveillance. It's only those who are dissidents, who challenge power, who have something to worry about. There all kinds of reasons why we should want to avoid that lesson as well. You may be a person who, right now, doesn't want to engage in that behavior, but at some point in the future you might. Even if you're somebody who decides that you never want to, the fact that there are other people who are willing to and able to resist and be adversarial to those in power – dissidents and journalists and activists and a whole range of others – is something that brings us all collective good that we should want to preserve."

Edward Snowden, in a conversation organized by the Tor Project[219]:

"This kind of tracking and tracing of human populations at scale will ultimately lead... You're not going to feel the consequences of it today. When we're talking about the internet, when we're talking about surveillance, we are talking about power. They're not spying on our records, they're not monitoring your traffic because it's interesting to them, they're not doing this for fun. They're not interested in data for data's sake, you know these are not academics they're not performing a study. They're doing it because it provides them influence. It allows

“Saying that you don’t care about privacy because you have nothing to hide is no different from saying you don’t care about freedom of speech because you have nothing to say. Or that you don’t care about freedom of the press because you don’t like to read.”

Edward Snowden

them to shape your behavior. It allows them to show you something that you wouldn’t have otherwise seen that they think you will click on, which will nudge and direct – or misdirect – your behavior, hopefully in the future. And it’s not gonna work every time. A thousand times it’s not gonna work but on that thousand and first time it will. And bit by bit they begin to control the individual, and through the individual they control the community, and through the community they influence the society. And then we are captured. And when I say you will not feel the consequences today, people go ‘I don’t care, it doesn’t matter, I’m not looking at anything interesting’. You are forgetting that when you say, you’re making yourself vulnerable to a system that never forgets. You are effectively making a bet that if you don’t matter today, if you don’t have anything interesting to say today, if you don’t have anything provocative or controversial to say, if you

are not in the minority today – you never will be. But you don't know what tomorrow looks like. You don't know what society looks like tomorrow. These systems, governmental and corporate, are trying to create what they call 'frictionless' systems. What they mean by that is front-loading the joy, getting you the pictures you want, the connections that you want, those endorphin hits, the dopamine that you want. And they are back-loading the consequences. They're hiding it, they're concealing it. And you won't learn about it for 5 years, for 10 years, for 20 years. But then once you do learn about it, it's too late to unring that bell, it's too late to protect yourself."

Ultimately, 'I have nothing to hide' is completely irrelevant in the discussion about mass surveillance. Because it's not just about you. Personal privacy is a human right and there are people all over the world who don't have the luxury of reasoning in terms of whether or not they have anything to hide, because they live under constant oppression. Fighting for privacy means fighting for them, here and now. And to make sure that everyone who doesn't yet live under totalitarian powers won't one day end up there. As Edward Snowden writes in his book Permanent Record:

"Because a citizenry's freedoms are independent, to surrender your own privacy is really to surrender everyone's. You might choose to give it about a convenience, or under the popular pretext that privacy is only required by those who have something to hide. But saying that you don't need or want privacy because you have nothing to hide is to assume that no one should have, or could have, to hide anything – including their immigration status, unemployment history, financial history, and health records. You're assuming that no one, including yourself, might object to revealing to anyone information about their religious beliefs, political affiliations, and sexual activities, as casually as some choose to reveal their movie and music tastes and reading preferences.

Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say. Or that you don't care about freedom of the press because you don't like to read. Or that you don't care about freedom of religion because you don't believe in God. Or that you don't care about the freedom to peaceably assemble because you're a lazy, antisocial agoraphobe. Just because this or that freedom might not have meaning to you today doesn't mean that it doesn't or won't have meaning tomorrow, to you, or to your neighbor – or to the crowds of principled dissidents I was following on my phone who were protesting halfway across the planet, hoping to gain just a fraction of the freedoms that my country was busily dismantling."

"Just because this or that freedom might not have meaning to you today doesn't mean that it doesn't or won't have meaning tomorrow, to you, or to your neighbor – or to the crowds of dissidents halfway across the Earth, hoping to gain just a fraction of the freedoms that my country was busily dismantling."

Edward Snowden

NOTES

You can find all the links at mullvad.net

[1] Wired: Cambridge Analytica Could Have Also Accessed Private Facebook Messages

[2] BBC: Facebook's data-sharing deals exposed

[3] The New York Times: As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants.

[4] The Guardian: The Cambridge Analytica Files

[5] The New York Times: Facebook's Data Sharing and Privacy Rules: 5 Takeaways From Our Investigation.

[6] Signal.org

[7] The New York Review: "We Kill People Based on Metadata"

[8] Johns Hopkins University: The Price of Privacy: Re-Evaluating the NSA

[9] Contrachrome.com

[10] VPRO Documentary: Shoshana Zuboff on surveillance capitalism

[11] Contagious: Shoshana Zuboff on the age of surveillance capitalism

[12] The intercept: Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data

[13] The Guardian: Privacy no longer a social norm, says Facebook founder

[14] EFF: Google CEO Eric Schmidt Dismisses the Importance of Privacy

[15] Gawker.com: Google CEO: Secrets Are for Filthy People

[16] Business Insider: Google CEO: "We Know Where You Are. We Know Where You've Been. We Can More Or Less Know What You're Thinking About."

[17] Humanetech.com

[18] Thesocialdilemma.com

[19] The Harvard Gazette: High tech is watching you

[20] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[21] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[22] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[23] Daily Mail: To read, or not to read... the terms and conditions: PayPal agreement is longer than Hamlet, while iTunes beats Macbeth.

[24] The Washington Post: I tried to read all my app privacy policies. It was 1 million words.

[25] FTC: FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations.

[26] Time: The Most Important Things to Know About Apps That Track Your Location

[27] Bloomberg: Meta Signs $37.5 Million Deal Over Facebook Location Tracking

[28] Politico: Facebook parent company to settle Cambridge Analytica scandal lawsuit for $725M

[29] The Guardian: The Cambridge Analytica Files

[30] The Intercept: Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data

[31] Vice: Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document

[32] ProPublica: Facebook Doesn't Tell Users Everything It Really Knows About Them

[33] The Markup: Facebook Is Receiving Sensitive Medical Information from Hospital Websites

[34] Bleeping Computer: Misconfigured Meta Pixel exposed healthcare data of 1.3M patients

[35] CNBC: Meta fined over $400 million by top EU regulator for forcing users to accept targeted ads

[36] The Markup: How We Built a Real-time Privacy Inspector

[37] Bloomberg: Zuckerberg Says Facebook Collects Internet Data on Non-Users

[38] Sveriges Radio: Facebook collects intimate customer data from over 100 European pharmacies

[39] ProPublica: Facebook Doesn't Tell Users Everything It Really Knows About Them

[40] The Intercept: Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document

[41] Google Patents: US10149111B1

[42] Buzzfeed News: Facebook Filed A Patent To Calculate Your Future Location

[43] Bloomberg: Meta Sued for Skirting Apple Privacy Rules to Snoop on Users

[44] Techradar: Facebook reveals it can track users location even if they turn off location services

[45] The Guardian: The Cambridge Analytica Files

[46] Buzzfeed News: Here Are 18 Things You Might Not Have Realized Facebook Tracks About You

[47] Forbes: Security Researcher Finds Facebook App Tracking iPhone Movements

[48] The Guardian: Boot up: Facebook self-censorship, Tufte in brief, developer intention, and more.

[49] Daily Mail: Facebook can predict when you'll get married, change jobs and even DIE: Patents reveal the shocking algorithms the firm runs on its users

[50] The Markup: How We Built a Real-time Privacy Inspector

[51] Daily Mail: How Google is using fonts to track what you do online and sell data to advertisers - and what you can do about it

[52] Statista: Google's Search Dominance

[53] Statista: Global market share held by leading desktop internet browsers from January 2015 to December 2022

[54] Contrachrome.com

[55] The Guardian: Google will pay $392m to 40 states in largest ever US privacy settlement

[56] Chromeunboxed.com: Google Analytics banned in several European countries due to GDPR violations

[57] Politico: Washington wants to break up Google. But Europe is way ahead.

[59] EFF: Google's FLoC Is a Terrible Idea

[60] Time: Europe Is Saving Democracy From Big Tech, Says the Author of Surveillance Capitalism

[61] Wired: Google Will Delete Your Data by Default—in 18 Months

[62] The Washington Post: Okay, Google: To protect women, collect less data about everyone.

[63] The Washington Post: Google promised to delete sensitive data. It logged my abortion clinic visit.

[64] The Guardian: Google under scrutiny over pledge to protect abortion location data

[65] The Guardian: TikTok has been accused of 'aggressive' data harvesting. Is your information at risk?

[66] TikTok.com: Privacy Policy

[67] Wired: All the ways Amazon tracks you and how to stop it

[68] Business Insider: Amazon is introducing new tech to monitor shoppers in its grocery stores and share data with advertisers

[69] Forbes: Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data

[70] Wired: Forget Facebook, mysterious data brokers are facing GDPR trouble.

[71] The Markup: The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users

[72] FTC: FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations.

[73] Vice: Data Broker Is Selling Location Data of People Who Visit Abortion Clinics

[74] Time: The Most Important Things to Know About Apps That Track Your Location

[75] Worldprivacyforum.org: Congressional Testimony: What Information Do Data Brokers Have on Consumers?

[76] CBS News: The Data Brokers: Selling your personal information

[77] ProPublica: Facebook Doesn't Tell Users Everything It Really Knows About Them

[78] Wired: It's time to ditch Chrome

[79] Reuters: Google faces $5 billion lawsuit in U.S. for tracking 'private' internet use

[80] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[81] The Tor Project: Browser Fingerprinting: An Introduction and the Challenges Ahead

[82] The Guardian: Boot up: Facebook self-censorship, Tufte in brief, developer intention, and more.

[83] Arvind Narayanan and Vitaly Shmatikov, The University of Texas at Austin: Robust De-anonymization of Large Sparse Datasets.

[84] Latanya Sweeney, Harvard University: Matching Known Patients to Health Records in Washington State Data.

[85] Techcrunch: Researchers spotlight the lie of 'anonymous' data

[86] Nature.com: Unique in the Crowd: The privacy bounds of human mobility

[87] Science.org: Unique in the shopping mall: On the reidentifiability of credit card metadata

[88] United Nations: Universal Declaration of Human Rights

[89] LeakSourcetv: CIA's Chief Tech Officer on Big Data: We Try to Collect Everything and Hang Onto It Forever

[90] The Guardian: Welcome to Utah, the NSA's desert home for eavesdropping on America

[91] Center for democracy & technology: Section 702: What It Is & How It Works

[92] The Guardian: NSA collecting phone records of millions of Verizon customers daily

[93] The Guardian: NSA collects millions of text messages daily in 'untargeted' global sweep

[94] The Guardian: XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

[95] The Guardian: XKeyscore presentation from 2008 – read in full

[96] The Guardian: All the data about your data

[97] The Washington Post: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

[98] ABC News: Dissecting Big Tech's Denial of Involvement in NSA's PRISM Spying Program

[99] EFF: Upstream vs. PRISM

[100] The New York Times: AT&T Helped U.S. Spy on Internet on a Vast Scale

[101] The Guardian: Glenn Greenwald: how the NSA tampers with US-made internet routers

[102] The New York Review: 'We Kill People Based on Metadata'

[103] Citizenfourfilm.com

[104] Theintercept.com/staff/glenn-greenwald/

[105] Reuters: Snowden says NSA engages in industrial espionage: TV

[106] The Guardian: Edward Snowden: US government spied on human rights workers

[107] Le Monde: France in the NSA's crosshair : phone networks under surveillance

[108] The Guardian: NSA monitored calls of 35 world leaders after US official handed over contacts

[109] Wikipedia: Global surveillance disclosures (2013–present)

[110] WikiLeaks: Vault 7: CIA Hacking Tools Revealed

[111] Vice: The CIA Spied on People Through Their Smart TVs, Leaked Documents Reveal

[112] The Guardian: 'No regrets,' says Edward Snowden, after 10 years in exile

[113] The Guardian: States haven't stopped spying on their citizens, post-Snowden – they've just got sneakier.

[114] Wired: A simple guide to GCHQ's internet surveillance programme Tempora

[115] Amnesty: Why we're taking the UK government to court over mass spying

[116] The Guardian: GCHQ taps fibre-optic cables for secret access to world's communications

[117] The Guardian: GCHQ taps fibre-optic cables for secret access to world's communications

[118] Forbes: NSA Responds To Snowden Claim That Intercepted Nude Pics 'Routinely' Passed Around By Employees

[119] The Guardian: GCHQ's mass data interception violated right to privacy, court rules

[120] The Guardian: NSA surveillance exposed by Snowden was illegal, court rules seven years on.

[121] Politico: Europe's state of mass surveillance

[122] Noyb: CJEU declares Meta's GDPR approach illegal.

[123] France24: Critics claim Paris using 2024 Games to introduce Big Brother video surveillance

[124] Freedom House: Hungary

[125] Mullvad.net/chatcontrol

[126] The Verge: The UK's tortured attempt to remake the internet, explained.

[127] The Guardian: The Pegasus Project

[128] The Guardian: A data 'black hole': Europol ordered to delete vast store of personal data

[129] Freedom House: Countering an Authoritarian Overhaul of the Internet

[130] The Intercept: Hacked Documents: How Iran Can Track and Control Protesters' Phones

[132] The New York Times: When Nokia Pulled Out of Russia, a Vast Surveillance System Remained

[133] Wired: Inside Safe City, Moscow's AI Surveillance Dystopia

[134] The Washington Post: Russia's surveillance state still doesn't match China. But Putin is racing to catch up.

[135] The New York Times: How Investigative Journalism Flourished in Hostile Russia

[136] Wikipedia: Mass surveillance

[137] Freedom House: Explore the map

[138] South China Morning Post: How China's surveillance state was a mirror to the US for whistle-blower Edward Snowden

[139] CNBC: China has launched another crackdown on the internet — but it's different this time

[140] The Verge: Chinese authorities admit they're able to retrieve deleted WeChat messages

[141] Time: These Are the Countries Where Twitter, Facebook and TikTok Are Banned

[142] The New York Times: China's Surveillance State Is Growing. These Documents Reveal How.

[143] The Guardian: The great firewall of China: Xi Jinping's internet shutdown

[144] The Guardian: The great firewall of China: Xi Jinping's internet shutdown

[145] The Washington Post: China harvests masses of data on Western targets, documents show

[146] Freedom House: China

[147] Human Rights Watch: China: Police 'Big Data' Systems Violate Privacy, Target Dissent

[148] The New York Times: Four Takeaways From a Times Investigation Into China's Expanding Surveillance State

[149] The New York Times: China's Surveillance State Is Growing. These Documents Reveal How.

[150] BBC: AI emotion-detection software tested on Uyghurs

[151] Sveriges Radio: Facebook collects intimate customer data from over 100 European pharmacies

[152] The Markup: The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users

[153] FTC: FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations

[154] FTC: A Look At What ISPs Know About You.

[155] BBC: Facebook's data-sharing deals exposed

[156] FTC: Big Data. A tool for inclusion or exclusion?

[157] The Washington Post: Health apps share your concerns with advertisers. HIPAA can't stop it.

[158] The Washington Post: Top U.S. Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars

[159] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[160] World Privacy Forum: Congressional Testimony: What Information Do Data Brokers Have on Consumers?

[161] Wired: The complicated truth about China's social credit system

[162] Wired: The complicated truth about China's social credit system

[163] Newsweek: 'Black Mirror' in China? 1.4 Billion Citizens to Be Monitored Through Social Credit System

[164] Wikipedia: Nosedive (Black Mirror)

[165] The Guardian: How private is your period-tracking app? Not very, study reveals

[166] The New York Times: The Privacy Project

[167] The New York Times: How to Track President Trump

[168] Vice: Data Broker Is Selling Location Data of People Who Visit Abortion Clinics

[169] Time: Supreme Court Allows Texas Abortion Law to Stand, But Says Abortion Providers Can Challenge It.

[171] The New York Times: We Need to Take Back Our Privacy

[172] Wired: The Case of the Creepy Algorithm That 'Predicted' Teen Pregnancy

[173] The Washington Post: Okay, Google: To protect women, collect less data about everyone.

[174] The Intercept: Hacked Documents: How Iran Can Track and Control Protesters' Phones

[175] BBC: Iran installs cameras to find women not wearing hijab

[176] The New York Times: When Nokia Pulled Out of Russia, a Vast Surveillance System Remained

[177] Wired: Inside Safe City, Moscow's AI Surveillance Dystopia.

[178] CNBC: China has launched another crackdown on the internet — but it's different this time.

[179] The Guardian: The great firewall of China: Xi Jinping's internet shutdown

[180] The New York Times: How China's Police Used Phones and Faces to Track Protesters

[181] Technology Review: This huge Chinese company is selling video surveillance systems to Iran

[182] Human Rights Watch: China: Phone Search Program Tramples Uyghur Rights

[183] CNN: Watched, judged, detained.

[184] BBC: AI emotion-detection software tested on Uyghurs

[185] BBC: AI emotion-detection software tested on Uyghurs

[186] The Guardian: The Pegasus Project

[187] Wikipedia: Nineteen Eighty-Four

[188] Wikipedia: Brave New World

[189] Humanetech.com: democratic functioning

[190] Humanetech.com: democratic functioning

[191] The Intercept: Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document.

[192] Humanetech.com

[193] Thesocialdilemma.com

[194] Jordanharbinger.com: 156: Why You Should Unplug from Social Media for Good

[195] Thesocialdilemma.com

[196] VPRO documentary: Shoshana Zuboff on surveillance capitalism

[197] Wired: Get Ready for the Next Big Privacy Backlash Against Facebook

[198] The Guardian: Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy'

[199] Humanetech.com: democratic functioning

[200] Massachusetts Institute of Technology: Study: On Twitter, false news travels faster than true stories.

[201] NBC News: 'Carol's Journey': What Facebook knew about how it radicalized users

[202] Amnesty: 'The Great Hack': Cambridge Analytica is just the tip of the iceberg

[203] The Guardian: Cambridge Analytica: how did it turn clicks into votes?

[204] BBC: 'Cambridge Analytica planted fake news'

[205] The Guardian: Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles'

[206] Amnesty: 'The Great Hack': Cambridge Analytica is just the tip of the iceberg

[207] The New York Times: Russians Again Targeting Americans With Disinformation, Facebook and Twitter Say

[208] Wikipedia: Cambridge Analytica

[209] VPRO Documentary: Shoshana Zuboff on surveillance capitalism

[210] Ted Talks: Why privacy matters

[211] Cigionline: Shoshana Zuboff on the Undetectable, Indecipherable World of Surveillance Capitalism.

[212] Universal Pictures All-Access: Snowden - Nothing To Hide, Nothing To Fear

[213] Ted Talks: Why privacy matters

[214] Npr.org: Ben Franklin's Famous 'Liberty, Safety' Quote Lost Its Context In 21st Century

[215] Wired: The Eternal Value of Privacy

[216] Schneier.com: The Eternal Value of Privacy

[217] Amnesty: Edward Snowden: 'Privacy is for the powerless'

[218] Ted Talks: Why privacy matters

[219] The Tor Project: PrivChat #3 - Advancing Human Rights with Tor

[221] The Register: Egyptian government caught tracking opponents and activists through phone apps

[222] Amnesty: Morocco: Human Rights Defenders Targeted with NSO Group's Spyware

[223] Wired: The FBI just admitted it bought US location data

[224] Wired: How the Pentagon learned to use targeted ads to find its targets – and Vladimir Putin

[225] Wall Street Journal: U.S. Spy Agencies Know Your Secrets. They Bought Them.

[226] Senator Ron Wyden: Wyden Releases Documents Confirming the NSA Buys Americans' Internet Browsing Records

[227] Electronic Frontier Foundation: Bad Amendments to Section 702 Have Failed

[228] Zwillgen: House Intelligence Committee FISA "Reform" Bill Would Greatly Expand the Class of Businesses and Other Entities Required to Assist in FISA 702 Surveillance

[229] The New York Times: Secret Rift Over Data Center Fueled Push to Expand Reach of Surveillance Program

[230] Senator Ron Wyden: "I Will Do Everything In My Power" to Stop Bill Expanding Government Surveillance Under FISA 702

[231] Edward Snowden on X/Twitter: The NSA is just days from taking over the internet, and it's not on the front page of any newspaper--because no one has noticed.

[236] IMDB: Total Trust

[237] Wikipedia: 709 Crackdown

[238] Wikipedia: Huang Xueqin

[239] IMDB: Total Trust

[240] Reuters: Google hit with 150 mln euro French fine for cookie breaches

[241] The Verge: Google will turn off third-party tracking for some Chrome users soon

[242] The Verge: Google abandons FLoC, introduces Topics API to replace tracking cookies

[243] Techradar: Facebook's Onavo VPN used to wiretap competitor data, court filings reveal

[244] patrick-breyer.de

[245] edps.europa.eu

[246] patrick-breyer.de

[247] patrick-breyer.de

[248] edri.org: Joint statement of scientists and researchers

[249] mullvad.net: The European Commission does not understand what is written in its own chat control bill

[250] Politico: Pegasus used by at least 5 EU countries, NSO Group tells lawmakers

[251] about.fb.com: Preventing child exploitation on our apps.

[252] Fokus: Chat Control: Så ska techjättarna skanna allt du skickar

[253] Fedpol 2021: Kampf gegen pädokriminalität

[254] edri.org: Uphold privacy, security and free expression by withdrawing new law

[255] patrick-breyer.de: Manipulative EU opinion poll no justification for indiscriminate chat control

[256] Balkaninsight: 'Who Benefits?' Inside the EU's Fight over Scanning for Child Sex Content

[257] Politico: The Qatargate files

[258] blog.cryptographyengineering.com

[259] The Intercept: New Group Attacking iPhone Encryption Backed by U.S. Political Dark-Money Network

[260] Engadget: Sex, lies, and surveillance: Something's wrong with the war on sex trafficking

[261] The Intercept: How Peter Thiel's Palantir Helped the NSA Spy on the Whole World

[262] The New York Times: Spy Contractor's Idea Helped Cambridge Analytica Harvest Facebook Data

[263] Netzpolitik: How the security apparatus shapes chat control

[264] Netzpolitik: Thorn also brought chat control into play for other topics

[265] Follow the money: Ashton Kutcher's anti childabuse software below par

[266] Balkaninsight: Europol Sought Unlimited Data Access in Online Child Sexual Abuse Regulation

[267] Wired: A Controversial Plan to Scan Private Messages for Child Abuse Meets Fresh Scandal

[268] europarl.europa.eu

[269] Fortune: Privacy-busting 'chat control' plans rejected by European Parliament as CSAM law heads into final stretch

[270] European court of human rights: case of podchasov v. Russia

[271] Reclaim the net: EU Officials Dodge Their Own Surveillance Law

[272] Netzpolitik: Behind closed doors

[273] data.consilium.europa.eu

[274] riksdagen.se

[275] patrick-breyer.de

[276] Netzpolitik: Why chat control is so dangerous

[277] Svenska Dagbladet: Expertkritik mot omstritt nätförslag i EU

[278] euractiv.com

[279] Aftonbladet: Mörkade allt för riksdagen

[280] europol.europa.eu: European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out

[281] polisen.se: Europas polischefer går samman mot grov brottslighet i en digital värld

[282] europol.europa.eu

[283] Svenska Dagbladet: Granskning: Poliser läcker till gängen

[284] Signal.org: AI, Encryption, and the Sins of the 90s

[285] The New York Times: Secret Documents Reveal N.S.A. Campaign Against Encryption

[286] CNN: U.S. enables Chinese hacking of Google

[287] IEEE: The Athens Affair

[288] blog.cryptographyengineering.com: remarks on “chat control”

[289] fbi.gov: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?

[290] EU Commission: Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement

[291] Wired: Microsoft’s Recall Feature Is Even More Hackable Than You Thought

[292] Netzpolitik: Going Dark – EU states want access to encrypted data and more surveillance

We live in a world where everything we do on the internet is tracked and saved. The tech giants say it openly: their goal isn't just to monitor everything you do, but to be able to predict your behavior. And to control it. And state agencies are no better. Instead of targeting their efforts, they carry out mass surveillance of the entire population. They break constitutional law without facing any consequences, and are discovered over and over again to be monitoring journalists, activists, and anyone who thinks differently to them.

We are already seeing how authoritarian countries use mass surveillance to control their inhabitants. In democracies, highly personal data has been collected and used in campaigns to influence elections. We are feeling the consequences of these actions, here and now. But the really big question is where we'll end up if we don't stop this abuse.

And to anyone saying they have nothing to hide – this isn't about you. It's about all our futures. About those who are vulnerable, and about our society. It's about the generations to come. About whether they will grow up in a free or controlling society.

MULLVAD VPN